5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI KRIPTOGRAFI ALGORITMA RSA UNTUK PENGAMANAN DATA ADMINISTRASI PADA KELURAHAN KREO BERBASIS *WEB*

Ahmad Sugali[1*], Pipin Farida Ariyani[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]1811503059@student.budiluhur.ac.id, [2*]pipin.faridaariyani@budiluhur.ac.id
(* : *corresponding author*)

Abstrak-Keamanan data merupakan aspek penting dalam pengelolaan informasi, terutama dalam lingkungan administrasi publik seperti pada kelurahan. Penerapan kriptografi menjadi solusi penting untuk memastikan kerahasiaan dan integritas data. Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi *Rivest Shamir Adleman* (RSA) berbasis web dalam pengamanan data administrasi di Kelurahan Kreo. Algoritma RSA dipilih karena kekuatannya dalam enkripsi dan dekripsi data melalui penggunaan kunci publik dan kunci privat. Metodologi penelitian meliputi perancangan sistem keamanan data berbasis web yang menggunakan algoritma RSA. Sistem ini dirancang untuk mengenkripsi data sensitif administrasi sebelum disimpan dan mendekripsi data saat diakses oleh pihak yang berwenang. Implementasi dilakukan dengan mengintegrasikan RSA dalam *framework web* yang ada, memastikan bahwa proses enkripsi dan dekripsi berjalan efisien tanpa mengurangi kinerja sistem. Hasil penelitian menunjukkan bahwa penerapan algoritma RSA dalam sistem berbasis web dapat meningkatkan keamanan data administrasi di Kelurahan Kreo. Data yang dienkripsi menjadi sulit diakses oleh pihak yang tidak berwenang, sementara pengguna yang sah tetap dapat mengakses informasi dengan cepat dan akurat melalui proses dekripsi yang efektif. Berdasarkan hasil pengujian dari penerapan proses enkripsi dan proses dekripsi dengan RSA didapatkan hasil yang baik dari hasil enkripsi yang tidak dapat dilihat orang yang tidak berhak dan hasil dekripsi yang tidak beda dengan *file* asli. Waktu yang di digunakan pada percobaan proses enkripsi dan dekripsi berbeda berdasarkan ukuran *file* (semakin besar ukuran *file* semakin lama proses enkripsi dan dekripsinya).

Kata Kunci: Kriptografi, Data, RSA, *Web*, Keamanan

IMPLEMENTATION OF RSA ALGORITHM CRYPTOGRAPHY FOR SECURING ADMINISTRATIVE DATA IN KREO DISTRICT WEB-BASED

Abstract- *Data security is an important aspect in information management, especially in public administration environments such as sub-districts. The application of cryptography is an important solution to ensure data security and integrity. This research aims to implement the web-based Rivest Shamir Adleman (RSA) cryptographic algorithm in securing data administration in Kreo Village. The RSA algorithm was chosen because of its strength in data encryption and decryption through the use of public keys and private keys. The research methodology includes designing a web-based data security system that uses the RSA algorithm. The system is designed to encrypt sensitive administrative data before it is stored and decrypt the data when accessed by authorized parties. Implementation is carried out by integrating RSA into the existing web framework, ensuring that the encryption and decryption processes run efficiently without reducing performance of the system. The research results show that the application of the RSA algorithm in a web-based system can improve the security of data administration in Kreo Village. Encrypted data becomes difficult for unauthorized parties to access, while authorized users can still access it quickly and accurately through an effective decryption process. Based on the test results of applying the encryption process and decryption process with RSA, good results were obtained from encryption results that could not be seen by unauthorized people and decryption results that were no different from the original files. The time used to test the encryption and decryption process varies based on the file size (the larger the file size, the longer the encryption and decryption process).*

Keywords*: Cryptography, Data, RSA, Web, Security*

1. PENDAHULUAN

Pesatnya kemajuan komputerisasi dan inovasi data semakin memudahkan kita dalam mengirim, menerima dan memperdagangkan informasi melalui media elektronik dengan cepat. Salah satu dampak buruk dari kemajuan inovasi data adalah pembobolan informasi [1]. Oleh karena itu penyebaran informasi sangatlah penting [2]. Kelurahan Kreo adalah satu bidang pelayanan publik yang dimana pelayanan administratif yang umum dilakukan adalah penandatanganan dokumen ataupun penginputan data diri dari masyarakat, hal ini menjadikan keamanan dan keaslian data menjadi tantangan.

Data dan informasi merupakan aset penting bagi dunia usaha dan individu, serta memiliki resiko pencurian dan penyalahgunaan dari pihak-pihak yang tidak bertanggung jawab [3]. Penyimpanan data menggunakan komputer agar melindungi data dan menjamin kerahasiaan data dan informasi berharga [4]. Masalahnya adalah pihak administrasi Kelurahan Kreo masih menyimpan data pada suatu *folder* pada computer tanpa adanya sistem pengamanan data. Apabila hal ini dibiarkan saja maka akan menimbulkan masalah karena bocornya data penting ke pihak yang tidak bertanggung jawab [5]. Oleh karena itu dibutuhkannya suatu cara yang dapat menjaga kerahasiaan informasi tersebut, yang salah satunya sering disebut dengan Kriptografi [6].

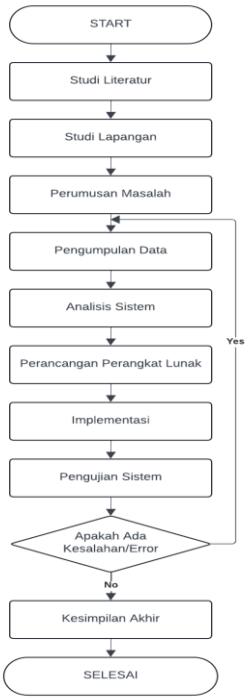
Kriptografi adalah seni dan ilmu melindungi data yang dikirimkan dengan mengubahnya menjadi kode tertentu dan membuatnya hanya dapat dilihat oleh mereka yang memiliki kunci untuk mengubah struktur kode tersebut kembali dan membantu menjaga kerahasiaan data atau pesan [7]. Kriptografi (kriptografi) datang dari bahasa Yunani, yaitu "cryptós" dan "gráphein" *Cryptós* artinya misterius, sedangkan *gráphein* artinya mengarang [8]. Proses pengubahan *ciphertext* menjadi *plaintext* disebut enkripsi, dan pada proses pengubahan *ciphertext* kembali menjadi *plaintext* disebut dekripsi [9].

Penelitian sebelumnya yang dilakukan oleh [10], Membahas Mengenai "Penerapan Algoritma Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung". Penelitian ini membahas mengenai penerapan sebuah sistem pengamanan dokumen yang berbasis web dengan menggunakan metode algoritma AES 256. Dalam penelitian sebelumnya ini orang yang menulis memakai algoritma AES 256 sedangkan dalam penelitian ini memakai algoritma RSA untuk mengamankan data pda Kelurahan Kreo.

Tujuan dari penelitian ini adalah agar mengetahui apakah Kriptografi Algoritma RSA berbasis Web pada data administrasi kelurahan kreo bermanfaat dalam keamanan data administrasi di kantor kelurahan tersebut. Algoritma yang digunakan adalah algoritma RSA (Rivest Shamir Addleman) dalam proses enkripsi serta proses dekripsi pada pengembangan sistem. RSA memakai perhitungan matematis yang cukup rumit dan melibatkan kunci keamanan awal (kunci pribadi atau kunci publik), sehingga sangat sulit dibobol oleh peretas [11]. RSA adalah perhitungan kriptografi *public key* yang paling terkenal. Pada tahun 1976, Ron Rivest, Adi Shamir, dan Leonard Adleman, tiga peneliti dari *Massachusetts Institute of Technology*, mengembangkan algoritma RSA. Sulitnya mengubah bilangan-bilangan besar menjadi faktor prima inilah yang menjadi kelebihan pada algoritma RSA [12].

2. METODE PENELITIAN

Metode penelitian ini digunakan sebagai gambaran langkah yang akan dilakukan pada penelitian ini agar penelitian tidak menyimpang dari tujuan awal. Hal ini diilustrasikan pada Gambar 1 di bawah yang menunjukkan langkah penelitian yang dilakukan.



Gambar 1. Penerapan Metode

2.1 Pengumpulan Data

Dalam fase ini, data dibutuhkan untuk merancang sistem keamanan dikumpulkan dengan beberapa fase yang dilakukan yang diantaranya adalah [13].

a. Studi Pustaka
Caranya dengan membaca jurnal, buku teks, dan referensi lain tentang teori kriptografi, teori keamanan data, teori RSA, dan teori penerapan sistem keamanan data ini.

b. *Interview*
Melakukan *interview* dengan pihak-pihak terkait, mengidentifikasi permasalahan terkini, dan membangun sistem yang dapat mengatasinya.

c. Pengamatan
Pengamatan dilakukan dengan cara melakukan pengamatan langsung pada bahan penelitian yang sebenarnya.

2.2 Metode Pengujian

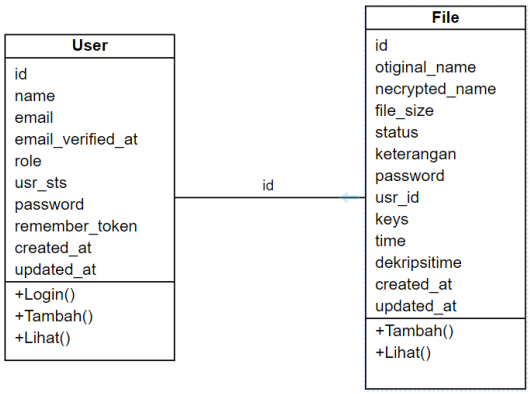
Rancangan pengujian yang akan dilakukan adalah menguji setiap fungsi – fungsi dari elemen yang ada pada aplikasi supaya diketahuin apakah sistem dalam aplikasi bekerja dengan baik.

2.3 Rancangan *Database*

Rancangan *Database* merupakan serangkaian proses perencanaan dan perancangan struktur serta skema penyimpanan data, guna memenuhi kebutuhan sistem informasi.

2.3.1 *Class Diagram*

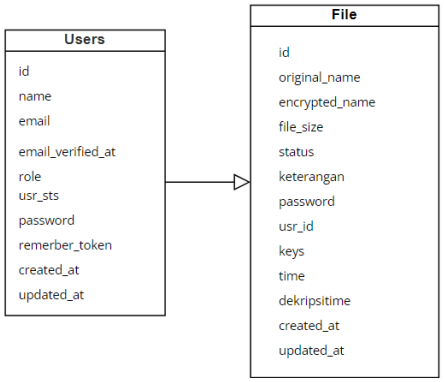
Class diagram yang digunakan seperti pada gambar 2 di bawah ini.



Gambar 2. *Class Diagram*

2.3.2 *Logical Record Structure* (LRS)

Logical Record Structure atau LRS yang di gunakan seperti pada gambar 3 di bawah ini.



Gambar 3. *Logical Record Structure* (LRS)

2.4 Kriptografi *Rivest Shamir Addleman* (RSA)

Algoritma enkripsi RSA adalah algoritma yang memfaktorkan bilangan yang sangat besar. dikarenakan alasan ini, RSA dianggap aman. Algoritma RSA dikembangkan pada tahun 1976 oleh tiga orang peneliti di *Massachusetts Institute of Technology:* Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Kelebihan algoritma RSA ini ialah usahnya menguraikan bilangan besar menjadi faktor prima. Oleh karena itu, semakin besar bilangan prima yang dipakai maka semakin aman algoritma tersebut. Enkripsi memakai algoritma RSA melibatkan 3 proses: pembuatan *public key/private key*, enkripsi, dan dekripsi. Untuk menghasilkan dua kunci, dipilih dua bilangan prima besar secara acak [14].

2.5 Proses Enkripsi RSA

Proses enkripsi Algoritma RSA diuraikan sebagai berikut:
a. Masukan *session key*, atau kunci publik
b. *Session Key* kemudian diubah menjadi bentuk ASCII
c. *Session Key* yang sudah diubah akan dienkripsi kembali dengan rumus:

$$ci = mi^e \ mod \ n \quad (1)$$

d. Dari langkah ketiga maka akan dihasilkan plainteks dalam bentuk ASCII
e. Ubah kembali bentuk ASCII menjadi karakter asli
f. Akan dihasilkan *session key* baru yang sudah dienkripsi [15].

2.6 Proses Dekripsi RSA

Proses dekripsi dapat diuraikan sebagai berikut :
a. Input *cipher key* atau *private key*
b. *Cipher key* akan diproses dengan rumus:

$$mi = ci^d \ mod \ n \quad (2)$$

c. Maka akan dihasilkan plainteks dalam bentuk ASCII
d. Plainteks tersebut bakal diubah dari bentuk ASCII menjadi karakter asli
e. *Session key* dihasilkan [15].

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Pertama menyiapkan dua komponen penting untuk implementasi: *software* serta *hardware*. Spesifikasi pada kedua komponen ini harus ditetapkan untuk membantu memastikan bahwa proses eksperimen berjalan dengan semestinya dan memberikan hasil yang diharapkan. Detailnya seperti di bawah ini:

3.1.1 Spesifikasi *Software*

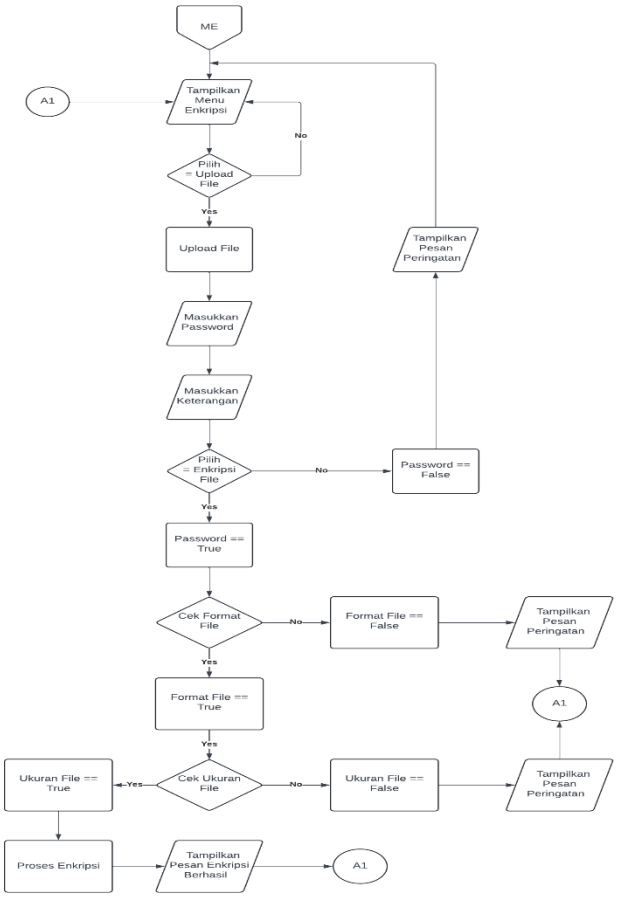
a. Sistem operasi *windows* 11 *pro*.
b. *Visual code editor*
c. *Browser google chrome*
d. XAMPP
e. *Balsamiq*

3.1.2 Spesifikasi *Hardware*

a. Komputer dengan *processor intel core* i7 12700k
b. RAM 32GB
c. SSD 1TB
d. *Mouse* dan *keyboard*

3.2 *Flowchart* Menu Enkripsi

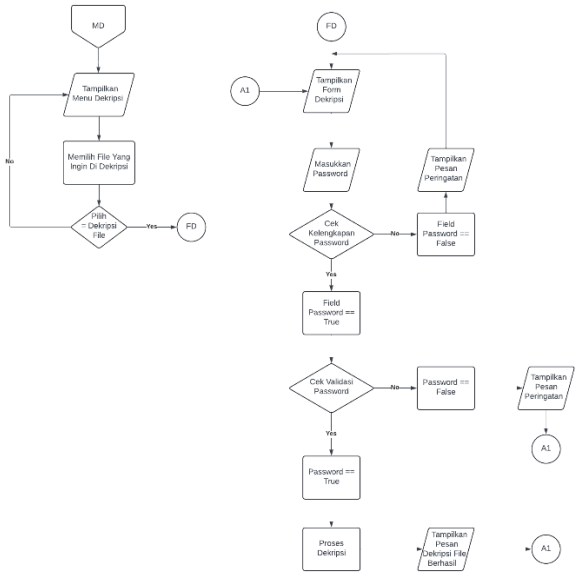
Pada *Flowchart* menu enkripsi ini merupakan alur proses dimana pengguna mulai dari mengupload *file* yang ingin di enkripsi serta memasukkan *password* dan keterangan untuk melakukan enkripsi file. Jika *file* yang di *upload* memenuhi syarat maka proses enkripsi dapat berjalan. *Flowchart* dari menu enkripsi seperti pada gambar 4 di bawah ini.



Gambar 4. *Flowchart* Menu Enkripsi

3.3 *Flowchart* Menu Dekripsi

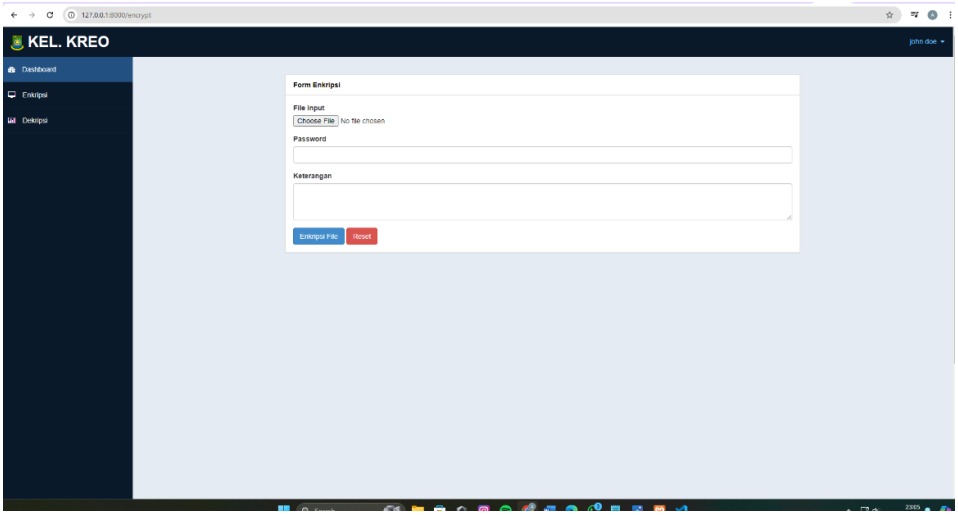
Fowchart menu dekripsi ini adalah *flowchart* yang menjelaskan tentang alur menu dekripsi. Di menu ini akan diperlihakan daftar dokumen yang sudah di enkripsi oleh pengguna bersamaan dengan informasi dari dokumen seperti no urutan dokumen, nama dokumen, sumber, nama dokumen enkripsi, path dokumen, status dokumen, dan aksi dekripsi. *Flowchart* dari menu dekripsi seperti pada gambar 5 di bawah ini.



Gambar 5. *Flowchart* Menu Dekripsi

3.4 Tampilan Layar Enkripsi

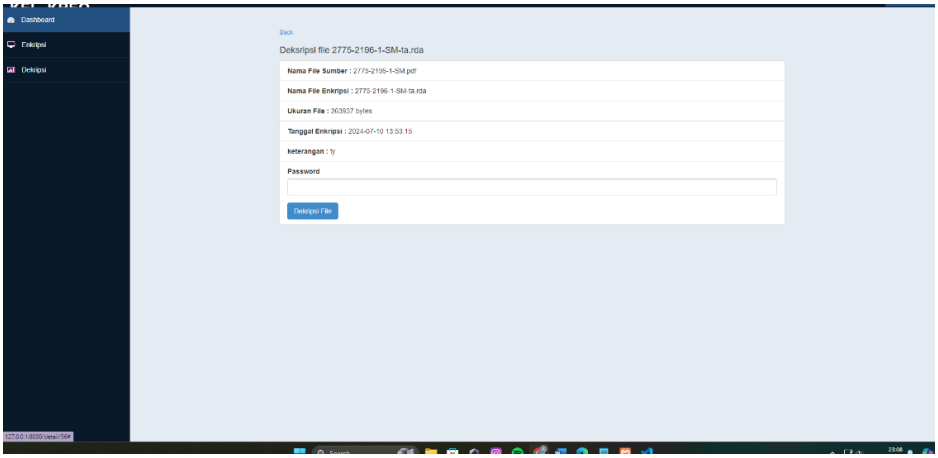
Setelah *login* dan mengakses *dashboard* ketuk menu Enkripsi untuk mengenkripsi file Anda, pengguna akan diminta untuk mengisi formulir enkripsi. Pengguna diharapkan memilih file yang ingin mereka enkripsi., akan tetapi ada Batasan tertentu, dimana file yang bias di enkripsi hanya file yang berformat docx, pptx, xlsx, pdf, dan txt, tampilannya seperti gambar 6 di bawah ini.



Gambar 6. Tampilan Layar Enkripsi

3.5 Tampilan Layar Dekripsi

Setelah Anda menekan tombol dekripsi, Anda akan diarahkan ke formulir dekripsi tempat Anda dapat memasukkan *password* dan melakukan proses dekripsi., tampilannya ada pada gambar 7 di bawah ini.



Gambar 7. Tampilan Form Dekripsi

3.6 Pengujian

Bagian ini merupakan tahap pengujian enkripsi dan dekripsi *file*. Tes ini membandingkan *file* yang tidak terenkripsi dengan *file* terenkripsi.

Table 1. Hasil Pengujian Enkripsi

No	Nama File Asli	Ukuran *File* Asli	Nama *File* Hasil Enkripsi	Ukuran *File* Hasil Enkripsi	Waktu Enkripsi	Status
1	ABSTRAK.docx	16359 B	ABSTRAK-ta.rda	29696 B	0.096 detik	BERHASIL
2	Surat Pengesahan.pdf	179725 B	Surat Pengesahan-ta.rda	322904 B	1.073 detik	BERHASIL
3	test.xlsx	120832 B	test-ta.rda	217088 B	0.72 detik	BERHASIL
4	tesstppt.pptx	248320 B	tesstppt-ta.rda	446124 B	1.475 detik	BERHASIL
5	BAB II Fix.pdf	258492 B	BAB II Fix-ta.rda	464556 B	1.571 detik	BERHASIL

Pada pengujian enkripsi, setelah serangkaian pengujian terkait proses enkripsi *file*, dapat dilihat bahwa adanya perubahan pada pengujian ukuran *file* selama proses enkripsi, dan proses enkripsi tidak memakan banyak waktu. Hal ini menunjukkan efisiensi dan konsistensi sistem dalam melakukan proses enkripsi pada varian *file* yang berbeda.

Table 2. Hasil Pengujian Dekripsi

No	Nama File Enkripsi	Ukuran *File* Enkripsi	Nama File Hasil Dekripsi	Ukuran *File* Hasil Dekripsi	Waktu Dekripsi	Status
1	ABSTRAK-ta.rda	29696 B	ABSTRAK.docx	16359 B	2.955 detik	BERHASIL
2	Surat Pengesahan-ta.rda	322904 B	Surat Pengesahan.pdf	179725 B	31.91 detik	BERHASIL
3	test-ta.rda	217088 B	test.xlsx	120832 B	21.434 detik	BERHASIL
4	tesstppt-ta.rda	446124 B	tesstppt.pptx	248320 B	44.63 detik	BERHASIL
5	BAB II Fix-ta.rda	464556 B	BAB II Fix.pdf	258492 B	46.425 detik	BERHASIL

Pada pengujian dekripsi, setelah serangkaian pengujian terkait proses enkripsi *file*, dapat dilihat bahwa tidak ada perubahan ukuran file dari ukuran file asli selama proses enkripsi, dan proses dekripsi memakan waktu yang relatif banyak.

4. KESIMPULAN

Menurut analisis dan uraian yang sudah dilakukan. Bisa disimpulkan bahwa algoritma *Rivest Shamir Adleman* (RSA) telah berhasil diimplementasikan pada aplikasi berbasis web yang dibuat dan mampu melindungi data dari pihak yang tidak berhak dan tidak bertanggung jawab. Pada aplikasi penulis, dokumen yang dienkripsi pada saat proses dekripsi terlihat sama dengan file sebelum dienkripsi. Waktu yang dibutuhkan untuk proses enkripsi dan dekripsi tergantung dengan besar kecilnya dokumen yang diproses (semakin kecil ukuran dokumen maka semakin cepat pula proses enkripsi dan dekripsinya; semakin besar ukuran dokumen maka semakin cepat pula proses enkripsi dan dekripsinya). Aplikasi berbasis website ini diharapkan nantinya bisa melakukan proses enkripsi dan dekripsi dengan ekstensi file selain xlsx, pptx, docx, txt. dan pdf. Pada penelitian selanjutnya disarankan untuk memakai algoritma RSA bersamaan dengan algoritma lain seperti AES.

DAFTAR PUSTAKA

[1] M. Rizky, P. F. Ariyani, "Penerapan Kriptografi Dengan Menggunakan Algoritma RSA Untuk Pengamanan Data Berbasis Dekstop Pada PT Trias Jaya Manunggal," *SKANIKA: Sistem Komputer dan Teknik Informatiak*, vol. 4, no. 2, pp. 77-82, 2021.

[2] H. N. Octaviana, A. Rosita, Implementasi Verifikasi Teks Menggunakan Metode Rivest Shamir Adleman (RSA), "*Jurnal ilmiah teknologi informasi terapan*", vol. 8, no. 1, pp. 72-77, 2021.

[3] N. Buulolo, A. Sindar, Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (*Data Encryption Standard*), "*J. RESPATI Jurnal Teknologi Informasi*", vol. 15, no. 3, pp. 61-65, 2020.

[4] K. Andriani, B. H. Hayadi, Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (RSA) Pada Toko Baju Family, "*Jurnal of Science and Social Research*", vol. 3, pp. 664-670, 2022.

[5] A. Thahara, I. T. Siregar, Implementasi Kriptografi untuk Keamanan Data dan Jaringan Menggunakan Algoritma DES, "*J. Jurnal Rekayasa Teknologi Informasi*", vol. 5, no. 1, pp. 31-38, 2021.

[6] H. Wijaya, Implementasi Kriptografi AES-128 Untuk Mengamankan URL (*Uniform Resource Locator*) Dari *SQL Injection*, "*J. AKADEMIKA*", vol. 7, no. 1, pp. 8-13, 2020.

[7] S. T. Siregar, N. B. Nugroho, H. Sigalingging, Implementasi Algoritma Kriptografi RSA (*Rivest Shamir Adleman*) Dalam Pengamanan Data Gaji Karyawan Di Kantor BSPJI, "*J. SAINTIKOM*" vol. 22, no. 2, pp. 528-538, 2023.

[8] Y. Suharya, H. Widia, Implementasi *Digital Signature* Menggunakan Algoritma Kriptografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay, "*J. Computing Jurnal Informatika*", vol 7, no. 1, pp. 20-29, 2020.

[9] I. Radianana, J. Jonathan, Implementasi Kriptografi engan Menggunakan Algoritma 3Des dan Algoritma RC4 Serta Kompresi Huffman Untuk Keamanan File, "*J. Technology of Information and Communication*", vol. 10, no. 3, pp. 159-168, 2022.

[10] I. K. Nurhareza, S. Siswanto, Penerapan Algoritma Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis *Web* Pada Kelurahan Belendung, "*J. SENAFTI*", vol. 1, no. 1, pp. 302-309, 2022.

[11] Yusfrizal, Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan RSA Berbasis Android, "*J. Teknik Informatika Kaputama*", vol.3, no. 2, pp. 29-37, 2019.

[12] A. Malvi, Painem, Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF), vol. 16, no. 2, pp. 67-74, 2020.

[13] A. S. Joel, F. Abdussalam, Y. Yunengsih, Tata Kelola Rekam Medis Berbasis Teknologi Informasi Dalam Penanganan Kerahasiaan Dan Keamanan Data Pasien Dengan Metode Kriptografi, "*J. Manajemen Informatika dan Komunikasi*", vol. 4, no. 3, pp. 837-848, 2023.
[14] M. Dairi, M. S. Asih, Khairunnisa, Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan, "*J. Ilmu Komputer dan Sistem Informasi*", vol. 2, no. 1, pp. 214-223, 2023.
[15] R. Siringoringo, Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File, "*J. KAKIFIKOM*", vol. 2, no. 1, pp. 31-42, 2020.