PENGAMANAN FILE REKAM MEDIS PADA PUSKESMAS LARANGAN UTARA MENGGUNAKAN ALGORITMA KRIPTOGRAFI RSA BERBASIS WEB

Reychan Davia Al Huday[1*], Sejati Waluyo[2]

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

Email: [1*]reychandavia1999@gmail.com, [2]sejati.waluyo@budiluhur.ac.id
(* : corresponding author)

Abstrak-Puskesmas Larangan Utara adalah unit pelayanan teknis yang menerima pelayanan kesehatan kepada pasien baru maupun pasien lama, *file* rekam medis setiap hari bertambah seiring banyaknya tindakan medis yang dibutuhkan pada Puskesmas Larangan Utara belum mendapat pengamanan yang lebih kepada rekam medis. *File* rekam medis hanya disimpan didalam sebuah ruangan yang sangat rentan untuk dicuri, hilang, atau data bisa diperjualbelikan oleh oknum yang tidak bertanggung jawab. Oleh karena itu, penelitian kali ini mempunyai tujuan untuk mengamankan *file* rekam medis yang terdapat di Puskesmas Larangan Utara. Dengan algoritma Rivest Shamir Adleman (RSA) dan ekstensi file yang lebih beragam seperti: *.docx, *.doc, *.xls, *.xlsx, *.pdf, *.txt pengamanan *file* rekam medis menjadi lebih mudah juga lebih aman dari pihak yang tidak bertanggung jawab. Metode ini dapat melakukan enkripsi dan dekripsi file terhadap rekam medis. Saat *file* dienkripsi dengan memasukkan dua buah bilangan prima, akan mengubah *file* rekam medis yang asli menjadi *file* yang tidak dapat dibaca dan membutuhkan kunci privat untuk membukanya. *File* dapat kembali ke bentuk asli jika dilakukannya dekripsi pada *file* tersebut. Dengan adanya aplikasi ini, maka proses penyimpanan data akan lebih aman untuk hasil enkripsi dengan rata-rata 0,014 dan untuk hasil dekripsi dengan rata-rata 1,614.

Kata Kunci: Kriptografi, Rivest Shamir Adleman, RSA, Rekam Medis, Enkripsi, Dekripsi.

SECURITY OF MEDICAL RECORDS AT PUSKESMAS LARANGAN UTARA USING WEB-BASED RSA CRYPTOGRAPHY ALGORITHM

Abstract- *Puskesmas Larangan Utara is a technical service unit that receives health services for new patients and old patients, the medical record files are increasing every day as the number of medical actions required at the Puskesmas Larangan Utara has not received more security for medical records. Medical record files are only stored in a room that is very vulnerable to being stolen, lost, or data that can be traded by irresponsible persons. Therefore, this study aims to secure the medical record files contained in the Puskesmas Larangan Utara. With the Rivest Shamir Adleman (RSA) algorithm and more diverse file extensions such as *.docx, *.doc, *.xls, *.xlsx, *.pdf, *.txt securing medical record files is easier and safer than irresponsible party. This method can encrypt and decrypt files on medical records. When a file is encrypted by entering two prime numbers, it will convert the original medical record file into an unreadable file and require a private key to open it. Files can return to their original form if they are decrypted. With this application, the data storage process will be more safer for encryption results with an average of 0,014 and for decryption results with an average of 1,614.*

Keywords*: Cryptography, Rivest Shamir Adleman, RSA, Medical Records, Encryption, Decryption.*

1. PENDAHULUAN

Keamanan data adalah faktor penting dalam sebuah pelayanan publik, khususnya dibidang Kesehatan. Karena dibidang Kesehatan, terdapat banyaknya data-data pasien yang bersifat sangat rahasia demi keamanan pasien tersebut. Sebagai salah satu contoh pada Puskesmas Larangan Utara. Ada permasalahan yang dimana pasien atau bahkan staff Puskesmas Larangan Utara masih belum mengetahui tentang keamanan data rekam medis tersebut. Jika ada rekam medis pasien yang bocor dan terjadi serangan pada system keamanan data, akan menimbulkan kerugian pada pasien dan Puskesmas Larangan Utara seperti penyalahgunaan data, pencurian data rekam medis pasien hingga penjualan data pasien.

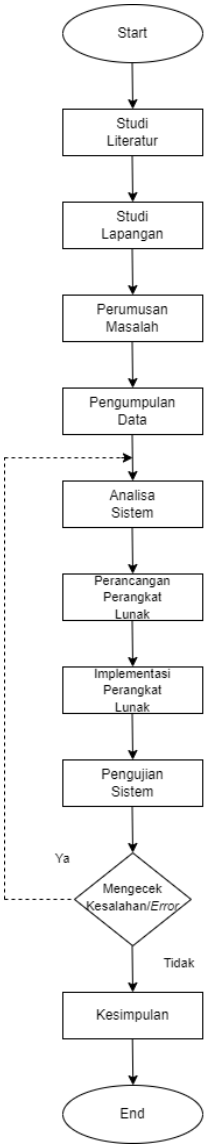
Rekam Medis adalah berkas berisi catatan dan dokumen tentang pasien yang berisi identitas, pemeriksaan, pengobatan, tindakan medis lain pada sarana pelayanan kesehatan untuk rawat jalan, rawat inap baik dikelola

pemerintah maupun swasta. Penyimpanan data rekam medis di Puskesmas Larangan Utara saat ini hanya mengandalkan pada *personal computer* dan brankas yang terdapat di Puskesmas Larangan Utara. Maka dari itu, sangat penting untuk instansi seperti puskesmas untuk mengamankan data rekam medis agar tidak disalahgunakan oleh orang yang tidak bertanggung jawab.

Kriptografi RSA adalah algoritma kriptografi asimetris yang menggunakan dua kunci yang berbeda untuk dekripsi dan enkripsi pesan. Kunci untuk enkripsi bersifat tidak rahasia atau bisa diketahui oleh siapa saja, dan kunci untuk dekripsi bersifat rahasia hanya diterima oleh pihak yang diberikan wewenang untuk membukanya. Berdasarkan uraian diatas, maka peneliti ingin melakukan pengembangan untuk membuat aplikasi pengamanan data rekam medis. Penelitian ini bertujuan untuk membuat keamanan tambahan yang lebih baik terhadap data rekam medis pasien.

2. METODE PENELITIAN

Metode penelitian digunakan sebagai pedoman dalam pelaksanan penelitian agar hasil yang akan dicapai tidak menyimpang dari tujuan yang telah dilakukan sebelumnya. Pada Gambar 1, merupakan tahapan yang dilakukan dalam penerapan metode penelitian yang akan dilakukan.



Gambar 1. Tahapan Penelitian

a. Studi Literatur
Pada metode ini yang akan dilakukan dengan mempelajari macam-macam jurnal, buku, dan karya ilmiah terdahulu yang topik pembahasannya berkaitan dengan masalah yang akan dibahas di penelitian ini.
b. Studi Lapangan
Pada studi lapangan, melakukan pengamanan terhadap *file* rekam medis pada Puskesmas Larangan Utara untuk dapat mengetahui permasalahan yang ada, dan melakukan perumusan masalah.
c. Perumusan Masalah
Pada perumusan masalah, masalah yang ditemukan dan akan diselesaikan dalam penelitian ini, berupa pengamanan file rekam medis untuk mencegah pencurian data, kebocoran data, dan jual beli data dari pihak yang tidak bertanggung jawab.
d. Pengumpulan Data
Pada pengumpulan data, dapat diperoleh berdasarkan wawancara, observasi, dokumen.
e. Analisa Sistem
Pengimplementasian perancangan pada sistem adalah proses enkripsi dan proses dekripsi pada *file* rekam medis yang selanjutnya akan disimpan ke database.
f. Perancangan Perangkat Lunak
Pada perancangan perangkat lunak, dilakukannya perancangan yang telah sesuai dengan analisis sistem terutama pada perancangan enkripsi dan dekripsi, serta hal lainnya yang di satukan ke dalam aplikasi.
g. Implementasi
Untuk penerapan pengamanan *file* rekam medis digunakan perangkat lunak seperti, Bahasa pemrograman PHP dan *Database Management System* (DBMS) yang menggunakan MySQL.
h. Pengujian Sistem
Pengujian pada sistem dilakukan guna memastikan sistem yang telah dibuat sesuat dengan hasil analisis dan perancangan sebelumnya.

2.1 Algorima Enkripsi dan Dekripsi

a. Algoritma Enkripsi

```
1.  Tampilkan Halaman Enkripsi
2.  Input File
3.  Input Kunci P dan Kunci Q
4.          If Kunci P dan Kunci Q == "True"
5.          If File == docx || doc || txt || xls || xlsx || pdf
6.          If nama file == "True"
7.                  Proses enkripsi
8.                  Direct halaman hasil enkripsi dengan kunci privat (D, N) dan
                    waktu .$duration. Detik
9.                          If pilih == Download
10.                         Download File Enkripsi
11.                         End if
12.                                 If pilih == Kembali
13.                                 Kembali ke baris 1
14.                                 End if
15.         Else
16.                 Tampilkan Pesan File yang dimasukan sudah dienkripsi
17.         End if
18.         Else
19.                 Tampilkan Pesan File yang dipilih tidak valid
20.         End if
21.         Else
22.             Direct Halaman Hasil Enkripsi dengan kunci privat (D, N) kosong dan
                waktu .$duration. Detik
23.             Kembali ke baris 1
24.         End if
```

Gambar 2. Tahapan Enkripsi

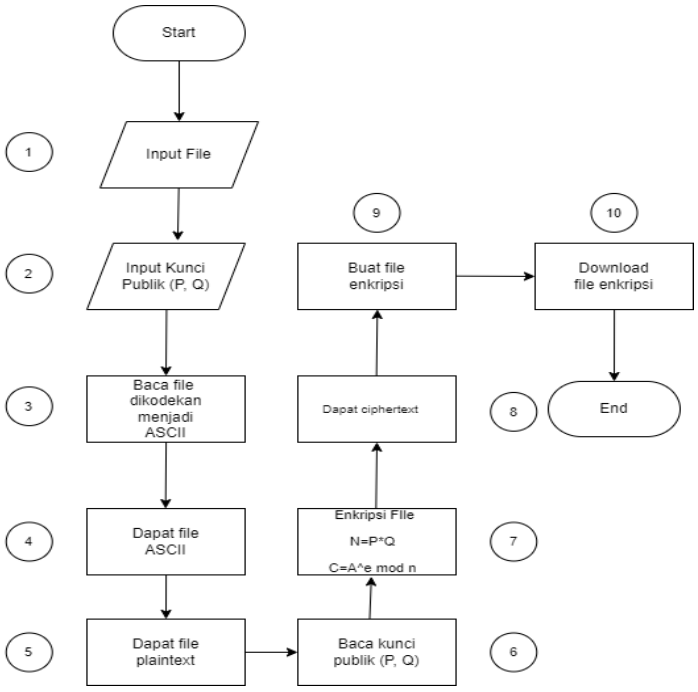
b. Algoritma Dekripsi

```
1.  Tampilkan Halaman Dekripsi
2.  Input file
3.  Input Kunci D dan Kunci N
4.          If Kunci D dan Kunci N == "True"
5.          If File == docx || doc || txt || xls || xlsx || pdf
6.          If nama file == "True"
7.                  Proses Dekripsi
8.                  Direct halaman hasil dekripsi dengan kunci privat (D, N) dan waktu .$duration.
                    Detik
9.                          If pilih == Download
10.                         Download File Dekripsi
11.                         End if
12.                                 if pilih == Kembali
13.                                 Kembali ke baris 1
14.                                 End if
15.         Else
16.                  Tampilkan Pesan File yang dimasukkan bukan hasil enkripsi
17.         End if
18.         Else
19.                  Tampilkan Pesan File yang dimasukkan bukan hasil enkripsi
20.         End if
21.         Else
22.                  Direct Halaman Hasil Dekripsi dengan kunci privat (D, N), file tidak berubah
                     menjadi plaintext dan waktu .$duration. Detik
23.                  Kembali ke baris 1
24.         End if
```

Gambar 3. **Tahapan Dekripsi**

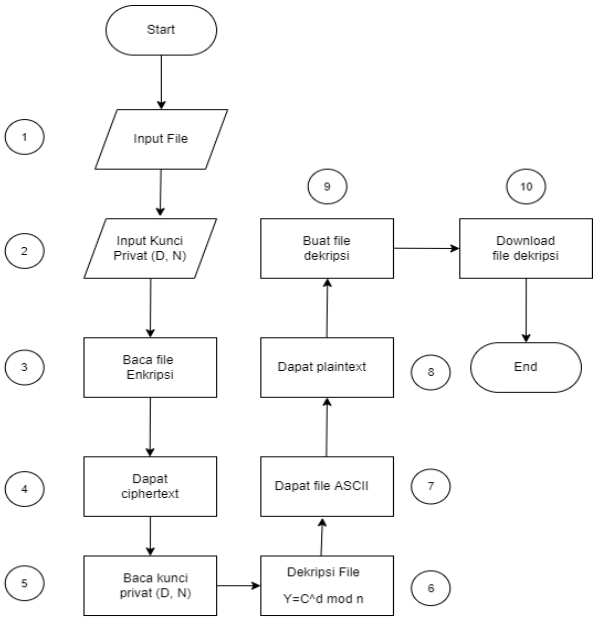
2.2 Metode Enkripsi dan Dekripsi RSA

a. Enkripsi RSA



Gambar 4. Enkripsi RSA

b. Dekripsi RSA



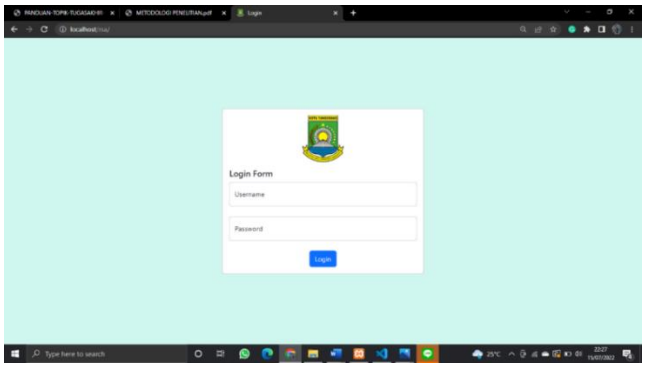
Gambar 5. Dekripsi RSA

3. HASIL DAN PEMBAHASAN

3.1 Tampilan Layar

a. Tampilan Layar Login

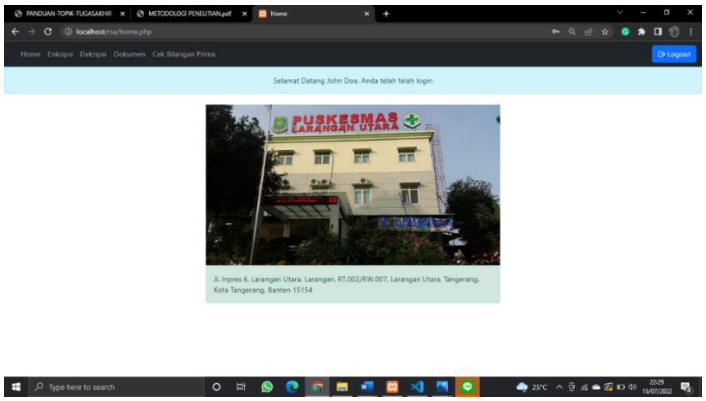
Berikut ini adalah Tampilan Layar Halaman Login. Pada halaman login pengguna diwajibkan untuk memasukkan *username* dan *password* untuk bisa mengakses halaman utama.



Gambar 6. Tampilan Layar Login.

b. Tampilan Layar Halaman Utama.

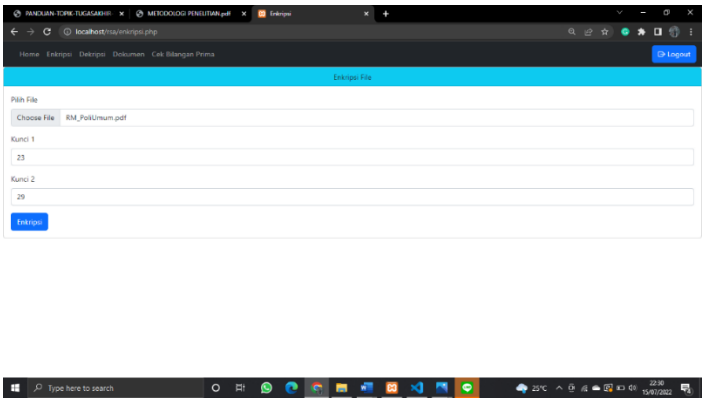
Tampilan layar halaman utama akan ditampilkan setelah proses dihalaman login. Pada halaman utama ini, pengguna akan melihat menu *Home*, Enkripsi, Dekripsi, Dokumen dan Cek Bilangan Prima.



Gambar 7. Tampilan Layar Halaman Utama.

c. Tampilan Layar Enkripsi

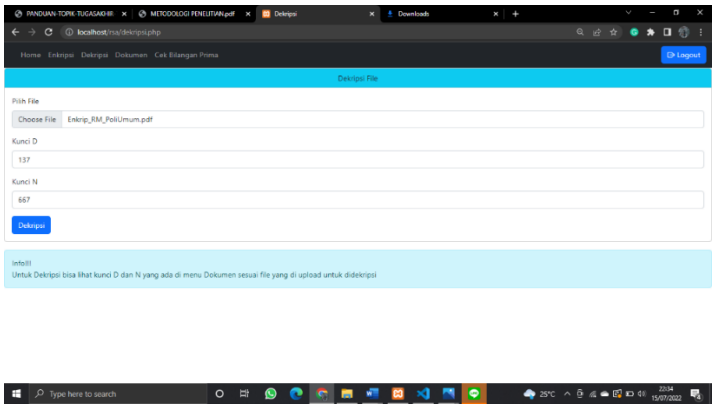
Pada tampilan layar enkripsi, pengguna dapat mengamankan data di menu ini. Dengan mengupload *file* yang ingin dienkripsi, dan memasukkan kunci 1 dan kunci 2 yang merupakan bilangan prima seperti yang terdapat pada Gambar 4.



Gambar 8. Tampilan Layar Enkripsi.

d. Tampilan Layar Dekripsi

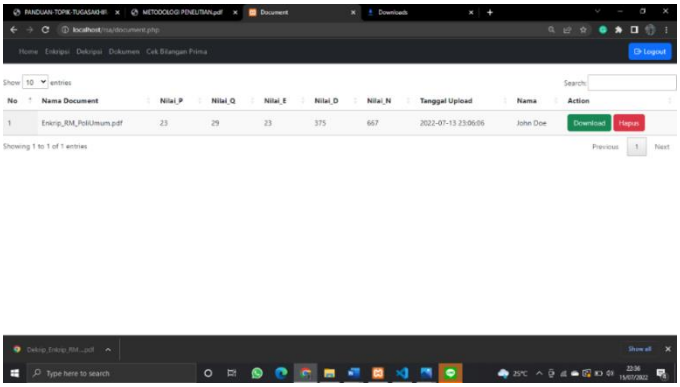
Berikut ini adalah merupakan tampilan layar menu dekripsi. Dimana, pengguna memasukkan *file* yang sebelumnya dienkripsi dan wajib memasukkan kunci privat seperti yang terdapat pada Gambar 5.



Gambar 9. Tampilan Layar Dekripsi.

e. Tampilan Layar Dokumen

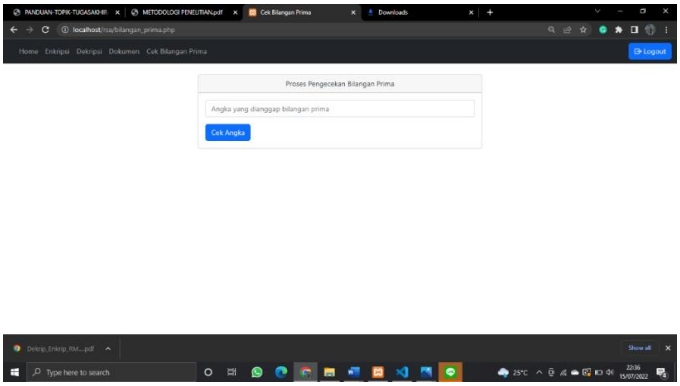
Berikut ini merupakan tampilan layar menu dokumen, pengguna dapat melihat *history file* yang telah dienkripsi, mengunduh ulang *file* hasil enkripsi dan menghapus *file* hasil enkripsi dari *database*.



Gambar 10. Tampilan Layar Dokumen.

f. Tampilan Layar Cek Bilangan Prima

Berikut ini merupakan tampilan layar pada menu cek bilangan prima, pengguna dapat mengecek bilangan prima seperti pada gambar.

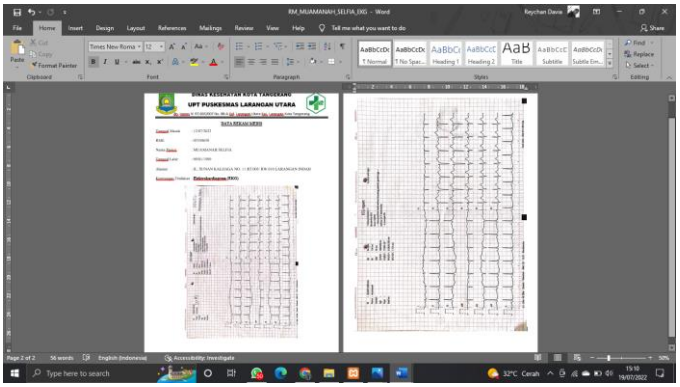


Gambar 11. Tampilan Layar Cek Bilangan Prima.

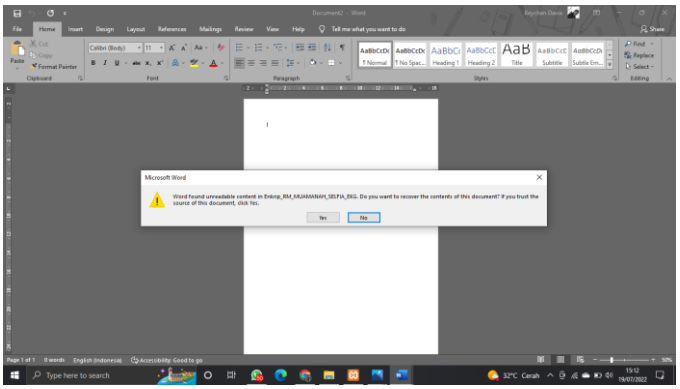
3.2 Analisis Hasil

Berikut ini merupakan hasil pengujian terhadap *file* asli (plaintext) dengan *file* yang telah dienkripsi. *File* yang akan di uji coba berupa *pdf, *docx.

a. Hasil pengujian *file* *docx terhadap plaintext dengan *file* yang berhasil dienkripsi.

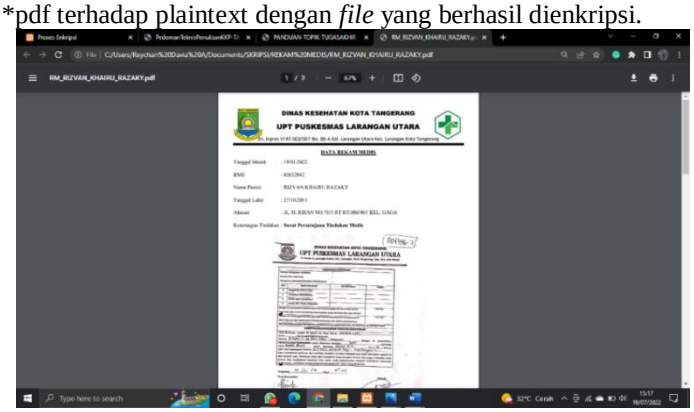


Gambar 12. *Plaintext file* *docx.

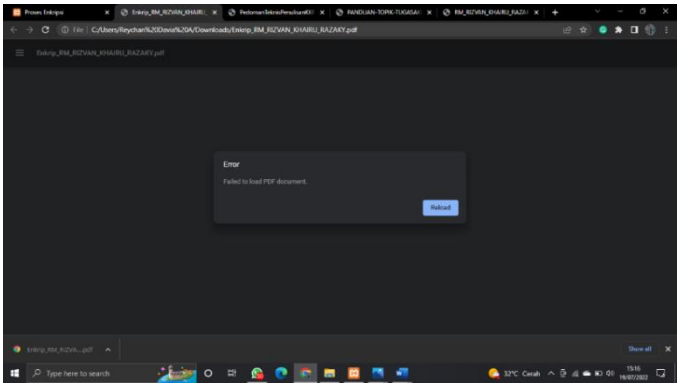


Gambar 13. Hasil Enkripsi *file* *docx.

b. Hasil pengujian *file* *pdf terhadap plaintext dengan *file* yang berhasil dienkripsi.



Gambar 14. ***Plaintext file* *pdf.**



Gambar 15. Hasil Enkripsi *File* *pdf.

3.3 Tabel Pengujian

Pada tabel pengujian, akan dibahas perbandingan pada proses enkripsi dan dekripsi file. File yang telah diuji meliputi *doc, *docx, *xlsx, *pdf. Untuk pengujiannya meliputi, ukuran file sebelum dan sesudah enkripsi, waktu proses enkripsi dan dekripsi.

Tabel 1. Tabel Pengujian Proses Enkripsi

Nama File Asli	Nama File Enkripsi	Ukuran File Asli	Ukuran File Enkripsi	Waktu Enkripsi (Detik)
RM_ENDE_HILMAN.docx	Enkrip_RM_ENDE_HILMAN.docx	351 KB	1,30 MB	0.0066812038421631

RM_RIZVAN_KHAIRU_RAZAKY.xlsx	Enkrip_RM_RIZVAN_KHAIRU_RAZAKY.xlsx	427 KB	1,56 MB	0.0053331851959229
RM_MUAMANAH_SELFIA_EKG.pdf	Enkrip_RM_MUAMANAH_SELFIA_EKG.pdf	726 KB	2,84 MB	0.038657903671265
RM_AYHUWAN_SELFI_EKG.doc	Enkrip_RM_AYHUWAN_SELFI_EKG.doc	367 KB	1,33 MB	0.0045838356018066

Tabel 2. Tabel Pengujian Proses Dekripsi

Nama File Enkripsi	Nama File Dekripsi	Ukuran File Enkripsi	Ukuran File Dekripsi	Waktu Enkripsi (Detik)
Enkrip_RM_ENDE_HILMAN.docx	Dekrip_Enkrip_RM_ENDE_HILMAN.docx	1,30 MB	350 KB	0.92558693885803
Enkrip_RM_RIZVAN_KHAIRU_RAZAKY.xlsx	Dekrip_Enkrip_RM_RIZVAN_KHAIRU_RAZAKY.xlsx	1,56 MB	426 KB	1.5480189323425
Enkrip_RM_MUAMANAH_SELFIA_EKG.pdf	Dekrip_Enkrip_RM_MUAMANAH_SELFIA_EKG.pdf	2,84 MB	763 KB	1.5553078651428
Enkrip_RM_AYHUWAN_SELFI_EKG.doc	Dekrip_Enkrip_RM_AYHUWAN_SELFI_EKG.doc	1,33 MB	367 KB	2.428316116333

Dari tabel pengujian proses enkripsi dan dekripsi diatas, dapat ditarik kesimpulan bahwa besar dan kecilnya ukuran sebuah *file* dapat mempengaruhi kecepatan proses enkripsi dan dekripsi. Isi *file* yang telah didekripsi tidak mengalami perubahan apapun.

3.4 Kelebihan Program

Berdasarkan hasil uji coba yang telah dilakukan, dapat ditarik kesimpulan kelebihan dari aplikasi tersebut yaitu:

a. Dengan tampilan antarmuka yang dibuat simple dan mudah dimengerti, pengguna dapat dengan mudah mengoperasikan aplikasi.
b. Dapat mengenkripsi *file* dengan lebih banyak extensi seperti *txt, *xls.
c. Isi *file* dokumen dengan extensi *docx, *doc, *pdf, *xlsx yang berhasil dienkripsi tidak dapat dibaca sebelum dilakukannya dekripsi.
d. *File* dokumen dengan extensi *docx, *doc, *pdf, *xlsx yang berhasil didekripsi tidak mengalami perubahan apapun terhadap isi dokumen.

3.5 Kekurangan Program

Berdasarkan hasil uji coba yang telah dilakukan, dapat ditarik kesimpulan kekurangan dari aplikasi tersebut yaitu:

a. Tidak dapat menambah jumlah pengguna.
b. Semakin besar ukuran *file*, semakin lama memakan waktu untuk melakukan proses enkripsi maupun dekripsi.
c. Tidak dapat melihat persentasi keamanan *file* setelah enkripsi.

4. KESIMPULAN

Berdasarkan pada penelitian yang telah dilakukan, dapat ditarik kesimpulan yang sejalan dengan penelitian:

a. Kriptografi mampu mengamankan data rekam medis dikarekan kriptografi merupakan teknis matematis yang berhubungan dengan aspek keamanan informasi yang menjaga kerahasiaan, integritas data, otentikasi dan menolak penyangkalan.
b. Algoritma Rivest Shamir Adleman (RSA) telah berhasil diimplementasikan dalam pengamanan rekam medis pada Puskesmas Larangan Utara. Cara melakukan pengamanan dalam Algoritma Rivest Shamir Adleman (RSA) tersebut dengan melakukan proses pembentukan kunci proses enkripsi, dan proses dekripsi.
c. Besarnya ukuran *file* dapat mempengaruhi kecepatan proses enkripsi dan dekripsi.

DAFTAR PUSTAKA

[1] S. Vivi Wahdini, D. Hartama, and I. Okta Kirana, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 3, pp. 101–107, 2021.
[2] M. D. A. Wicaksono, "Pengamanan Data Pelaut Menggunakan Algoritma Rivest Shamir Adleman (RSA) Pada PT. Bsm Csc Indonesia," *Seminar Nasional. Mahasiswa Ilmu Komput. dan Aplikasinya(SENAMIKA)*, UPN Veteran Jakarta, vol. 1, no. 1, pp. 17–24, 2020.
[3] A. Harbani and M. A. Fahreza, "Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop," *Teknois: Jurnal Ilmu Teknologi Informasi dan Sains*, vol. 9, no. 1, pp. 1–9, 2019.
[4] A. N. Agustina, Aryanti, and Nasron, "Pengamanan Dokumen Menggunakan Kombinasi Metode Rsa (Rivest Shamir Adleman) Dan Vigenere Cipher," *Prosiding Seminar Nasional Multi Disiplin Ilmu Call Paper UNISBANK*, pp. 14–19, 2017.
[5] M. Rizki and P. Farida Ariyani, "Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada PT. Trias Mitra Jaya Manunggal," *SKANIKA*, vol. 4, no. 2, pp. 1–6, 2021, doi: 10.36080/skanika.v4i2.1991.
[6] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018.
[7] B. Anwar, N. B. Nugroho, J. Prayudha, and A. Azanuddin, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 1, p. 30, 2019.
[8] S. Rahmadhiyanti, "Implementasi Kriptografi Rsa Untuk Peningkatan Keamanan Database E-Commerce," *Pelita Inform.*, vol. 8, no. 2, pp. 288-291, 2019.
[9] H. Santoso and M. Fakhriza, "Perancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma Rsa," *Algoritm. J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 47–54, 2018.
[10] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019.