

# **APLIKASI PENGAMANAN SURAT DENGAN METODE RC4 BERBASIS WEB DI KELURAHAN PAKUJAYA TANGERANG SELATAN**

**Safwah Setiono Puteri<sup>1\*</sup>, Sejati Waluyo<sup>2</sup>**

<sup>1,2</sup>Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: <sup>1\*</sup>safwahputeri@gmail.com, <sup>2</sup>sejati-waluyo@budiluhur.ac.id  
(\* : Corresponding Author)

**Abstrak-** pada abad ini, teknologi informasi semakin berkembang pesat. Sehingga dapat memudahkan banyak orang dalam melakukan kegiatan. Tak terkecuali instansi pemerintah daerah yaitu Kelurahan Pakujaya Tangerang Selatan yang memanfaatkan kemajuan teknologi untuk meningkatkan kinerja pelayanannya. Kelurahan Pakujaya menggunakan sistem yang bernama sisumaker untuk mengirimkan berbagai surat. Dengan pemanfaatan sistem tersebut ada berbagai dampak yang terjadi baik itu dampak positif maupun dampak negatif, dampak positif dari penggunaan sistem adalah pengiriman lebih efisien dan mempersingkat waktu. Dampak negatif yang terjadi adalah mudahnya terjadi pencurian data oleh pihak yang tidak memiliki hak terhadap data tersebut sebab belum adanya pengamanan terhadap *file* yang akan dikirim. Tujuan dari penelitian ini adalah membuat aplikasi guna mengamankan *file* dengan menggunakan metode algoritma kriptografi *Rivest Code 4 (RC4)*, dimana dalam pengamanan tersebut akan melalui proses enkripsi dan dekripsi. Dengan menggunakan metode *Rivest Code 4 (RC4)* ini akan memudahkan *user* dalam proses pengamanan *file* sebab algoritma RC4 merupakan algoritma simetris sehingga menggunakan kunci yang sama untuk enkripsi dan dekripsi. Aplikasi ini dikembangkan dengan menggunakan bahasa pemrograman PHP (*hypertext preprocessor*) dan MySQL yang digunakan untuk penyimpanan data. Hasil dari penelitian ini adalah aplikasi yang telah dirancang berjalan dengan baik serta ukuran *file* yang telah melalui proses enkripsi dan dekripsi tidak mengalami perubahan masih memiliki ukuran *file* yang sama dengan *file* aslinya.

**Kata Kunci:** Kriptografi, RC4, Aplikasi

## ***APPLICATION SECURITY OF MAIL USING RC4 METHOD WEB-BASED AT KELURAHAN PAKUJAYA TANGERANG SELATAN***

**Abstract-** *In this century, information technology is growing rapidly. So it can make easier for many people to do their activities. The local government agency, namely kelurahan Pakujaya , South Tangerang, is no exception, which utilizes technological advances to improve service performance. Kelurahan Pakujaya uses a system called sisumaker to send various letters. With the use of the system there are positive and negative impacts, the positive impact of using the system is more efficient delivery and shortening of time. The negative impact that occurs is that it is easy for data theft by irresponsible parties because there is no security for the files to be sent. The purpose of this study is to create an application to secure files using the Rivest Code 4 (RC4) cryptographic algorithm method, where the security will go through the encryption and decryption process. By using the Rivest Code 4 (RC4) method, it will make it easier for users in the process of securing files because the RC4 algorithm is a symmetric algorithm so it uses the same key for encryption and decryption. This application was developed using the PHP programming language (hypertext preprocessor) and MySQL which is used for database. The result of this research is that the application that has been designed runs well and the file size that has gone through the encryption and decryption process does not change, it still has the same file size as the original file.*

**Keywords:** *Cryptography, RC4, Application*

---

## **1. PENDAHULUAN**

pada abad ini teknologi informasi semakin berkembang pesat. Sehingga dapat memudahkan semua orang dalam melakukan kegiatan. Dengan perkembangan teknologi Informasi yang terjadi pada sekarang ini yang bergitu pesat sehingga sangat memudahkan setiap orang dalam mendapatkan pesan, data, ataupun informasi[1]. Salah satu kegiatan yang terpengaruh oleh perkembangan teknologi adalah kegiatan dalam berkomunikasi. Dengan berkembangnya teknologi dalam kegiatan komunikasi memudahkan kita dalam bertukar informasi. Namun meskipun banyak dampak positif dari berkembangnya teknologi informasi tidak menutup kemungkinan adanya dampak negatif dari hal tersebut. Salah satu dampak negatif yang dapat terjadi adalah adanya pencurian data informasi oleh pihak yang tidak bertanggung jawab. Dimana sekarang ini banyak sekali data informasi yang dicuri.

Selain adanya pencurian data informasi, penyalahgunaan data, serta pembajakan data pun sering terjadi. Seiring meningkatnya pencurian data, penyalahgunaan data, serta pembajakan data yang sangat merugikan bagi pihak yang memiliki data informasi tersebut, maka dengan adanya dampak negatif tersebut keamanan dalam pertukaran dan penyimpanan data informasi dianggap sangat penting. Karena suatu komunikasi jarak jauh belum tentu memiliki jalur yang aman. Tidak hanya permasalahan jalur yang dianggap kurang aman, penyimpanan data tersebut juga belum dapat dipastikan aman dari pencurian data informasi. Maka dari itu keamanan dalam dunia teknologi sangat dibutuhkan dan sangat penting. Kegiatan mengamankan sebuah data telah menjadi bagian terpenting dalam upaya menjaga kerahasiaan sebuah data, dimana data tersebut hanya boleh diketahui oleh pihak yang memiliki hak saja terhadap data tersebut, dan salah satu cara yang dapat dilakukan dalam menjaga kerahasiaan data tersebut dengan melakukan proses enkripsi dan dekripsi terhadap data untuk membuat data tersebut tidak dapat dibaca atau dimengerti oleh sembarang orang[2]. Guna tercapainya tujuan dalam menjaga kerahasiaan data informasi tersebut berbagai macam teknik keamanan telah dikembangkan yang bertujuan untuk melindungi serta menjaga kerahasiaan data agar terhindar dari pihak yang tidak berwenang atas data tersebut. Salah satu metode keamanan untuk mengamankan data adalah kriptografi.

Kriptografi adalah persamaan dari kata enkripsi yaitu dilakukannya penyandikan terhadap kata-kata yang awalnya ditulis dan dapat dipahami menjadi kata-kata atau kalimat yang tidak dapat dipahami[3]. Dalam kriptografi terdapat dua jenis kriptografi yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik merupakan tipe kriptografi dimana proses enkripsi dan dekripsinya dilakukan per karakter[4]. Kriptografi modern merupakan tipe kriptografi yang beroperasi dalam mode bit (dinyatakan dalam 0 dan 1)[4]. Metode dalam kriptografi memiliki langkah dan teknik pengamanan dengan cara yang berbeda-beda. Contoh metode yang dapat digunakan adalah RC4, dimana RC4 termasuk dalam algoritma simetris. Algoritma simetris merupakan algoritma yang melakukan proses enkripsi dan dekripsinya hanya terhadap satu blok data atau beroperasi dalam mode aliran (*stream cipher*)[5]. RC4 (*Rivest Cipher 4*) merupakan algoritma kriptografi yang termasuk *synchronous stream cipher* yang dimana memiliki kunci yang sama serta dalam proses enkripsi dilakukan secara digit per digit atau *byte per byte*[6]. Algoritma RC4 sudah secara umum digunakan untuk pembuatan aplikasi dan terbalik sangat aman sebab data yang dijaga dikirimkan melalui saluran komunikasi[7]. Metode algoritma RC4 menjadi metode algoritma tercepat dibandingkan dengan metode algoritma yang lainnya. Selain terdapat kelebihan algoritma RC4 juga terdapat kelemahan namun kelemahan tersebut dapat diatasi dengan cara memperbanyak bit junci serta dilakukannya perubahan dalam pengirisan K-Array[8]. Algoritma RC4 beroperasi dengan melalui metode XOR sehingga operasi enkripsi dengan XOR berlangsung sangat cepat oleh sebab itu RC4 sering digunakan bila diinginkan kecepatan yang memadai[9].

Kelurahan Pakujaya merupakan instansi pemerintah daerah yang berlokasi di Jl. Bhayangkara 1 No.78, Paku Jaya, Kec. Serpong Utara, Kota Tangerang Selatan, Banten. Di Kelurahan Pakujaya banyak tugas yang dilakukan oleh para staffnya salah satunya adalah tugas dalam pembuatan surat. Dalam pembuatan surat Kelurahan Pakujaya mengirimkan surat tersebut melalui sistem yang bernama sisumaker. Melalui sistem tersebut surat yang ingin dikirim menjadi lebih efisien menuju kepada penerima. Setelah melalui sisumaker, surat tersebut akan masuk ke dalam perangkat yang dituju baik komputer maupun *smartphone*. Namun penerima surat tersebut harus memantau perangkat mereka. Maka dari permasalahan diatas dirancangnya aplikasi pengamanan untuk mengamankan surat sebelum dikirimkan melalui sisumaker. Aplikasi yang dibuat dikembangkan dengan menggunakan Bahasa pemrograman PHP (*hypertext preprocessor*) dan menggunakan MySQL sebagai *database*. *Database* atau basis data sekumpulan data atau Informasi yang dimana data tersebut akan disimpan didalam sebuah sistem komputer dan dapat dilakukan perubahan pada data tersebut baik di edit maupun di hapus[10].

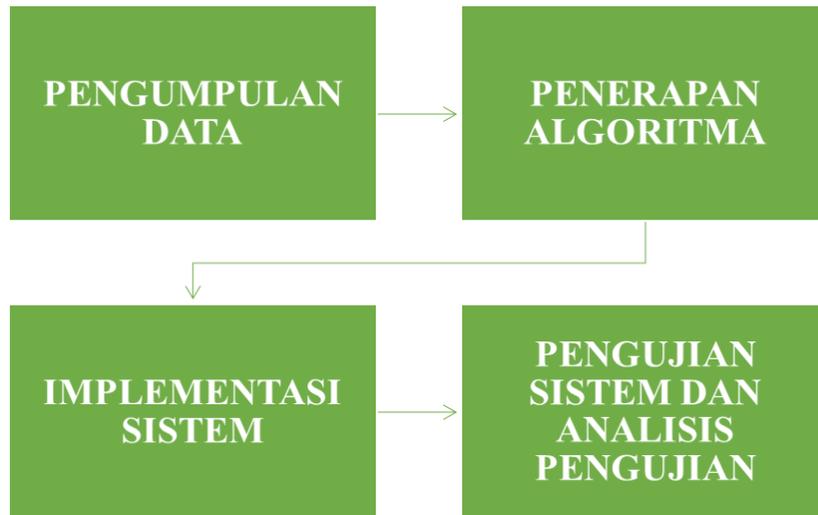
## 2. METODE PENELITIAN

### 2.1 Data Penelitian

Dalam penulisan penelitian ini, digunakan data yang ada pada sistem untuk dilakukannya penelitian di Kelurahan Pakujaya yang beralamatkan di Jl. Bhayangkara 1 No.78, Paku Jaya, Kec. Serpong Utara, Kota Tangerang Selatan, Banten. Data yang digunakan adalah *file* dalam bentuk *softcopy* yang di dapat melalui sisumaker.

### 2.2 Penerapan Metode

Pada tahapan penerapan metode yang digunakan sebagai acuan dalam dilakukannya penelitian sehingga penelitian yang dilakukan dapat berjalan sesuai rencana yang diinginkan. Berikut adalah tahapan yang dilakukan dalam penelitian:



Gambar 1. Penerapan Metode

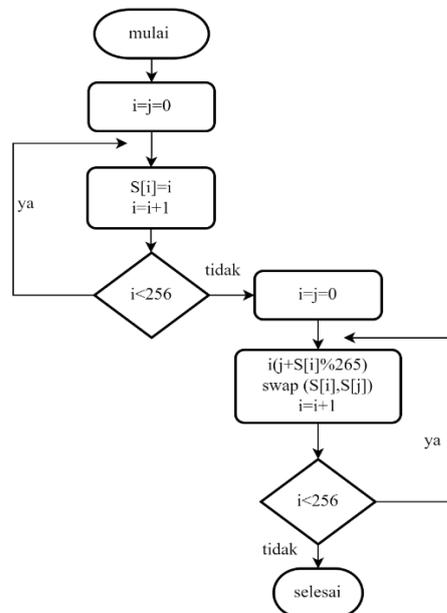
a. Pengumpulan Data

Proses pengumpulan data dilakukan dengan melalui proses wawancara dan melakukan observasi secara langsung di Kelurahan Pakujaya untuk mengetahui prosedur sistem yang ada di Kelurahan Pakujaya.

b. Penerapan Algoritma

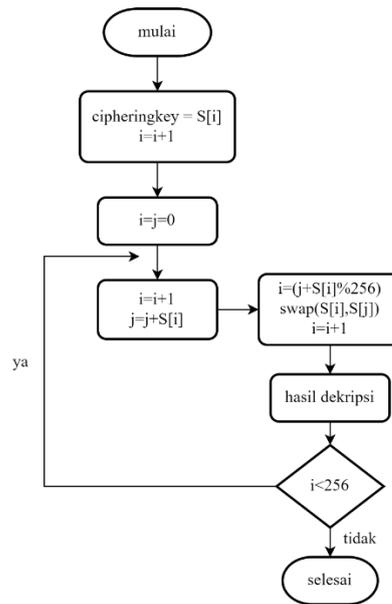
Permasalahan yang ada pada penelitian ini adalah diperlukannya sebuah aplikasi yang dapat digunakan untuk mengamankan *file* untuk tetap terjaga kerahasiaannya serta keamanannya. Aplikasi ini dirancang guna untuk mengamankan *file* dengan cara mengubah isi *file* tersebut menjadi kode yang tidak dapat dibaca dengan melalui proses enkripsi namun apabila *user* ingin mengembalikan *file* yang telah terenkripsi menjadi seperti semula dapat dilakukan dengan mendekripsi pesan. Dalam proses enkripsi dan dekripsi menggunakan algoritma kriptografi dengan metode RC4. Adapun proses enkripsi dan dekripsi menggunakan metode RC4 sebagai berikut:

1) Proses enkripsi dengan menggunakan metode RC4



Gambar 2. Proses Enkripsi

2) Proses dekripsi dengan menggunakan metode RC4



**Gambar 3.** Proses Dekripsi

c. Implementasi Sistem

Pada tahapan implementasi sistem dilakukannya pengimplementasian program dengan menggunakan Bahasa pemrograman PHP (*hypertext preprocessor*) serta menggunakan MySQL untuk penyimpanan data.

d. Pengujian Sistem dan Analisis Pengujian

Pada tahapan ini sistem yang ditelah dibuat akan diuji dengan menggunakan *black box* yang bertujuan untuk mengetahui apakah sistem sudah sesuai dengan yang telah dirancang dan sesuai kebutuhan, serta apakah aplikasi yang telah dibuat sesuai dengan yang diharapkan.

### 3. HASIL DAN PEMBAHASAN

#### 3.1 Implementasi Program

Berdasarkan program yang telah dibuat dengan menggunakan metode algoritma RC4 untuk mengamankan surat di Kelurahan Pakujaya, maka implementasi metode tersebut akan digambarkan seperti pada gambar dibawah ini:

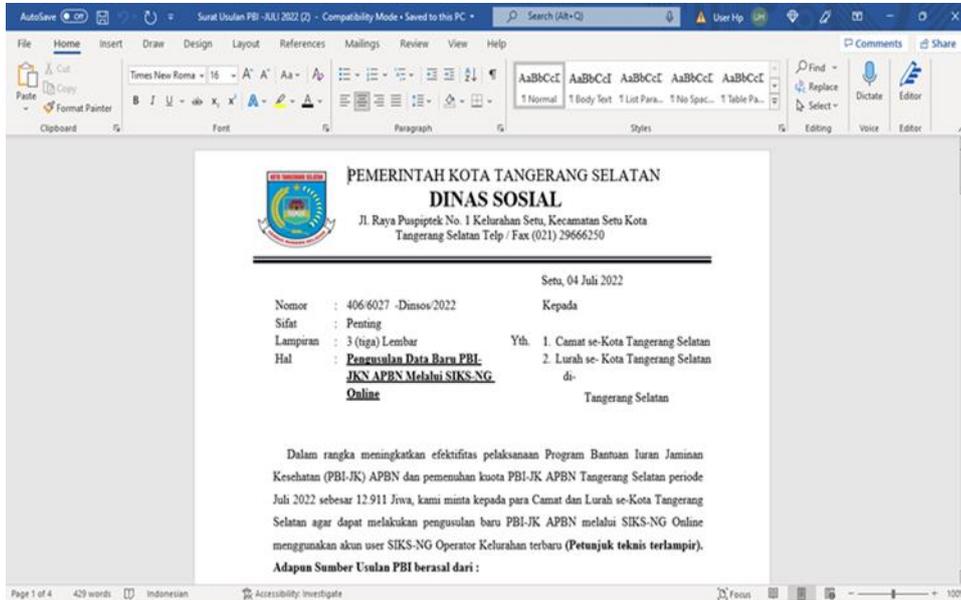
a. Enkripsi *file*

Pada tampilan layar halaman enkripsi terdapat *form* yang akan digunakan untuk mengenkripsi *file*. Sebelum melakukan proses enkripsi *user* harus memilih *file* yang akan di enkripsi terlebih dahulu, kemudian *user* akan diminta untuk memasukkan *password*, *password* minimal 8 karakter, lalu klik tombol enkripsi.



**Gambar 3.** Halaman Enkripsi

Apabila *user* telah memilih *file* dan memasukkan *password*, maka proses enkripsi dapat berjalan. Apabila proses enkripsi berhasil maka *file* yang telah terenkripsi akan masuk kedalam *database*. Berikut adalah gambaran *file* awal atau *file* yang belum terenkripsi.



Gambar 4. File Belum Terenkripsi

Berikut ini adalah gambaran *file* yang telah terenkripsi sehingga isi dari *file* tersebut akan berubah. Tampilan *file* setelah terenkripsi dapat dilihat pada gambar:



Gambar 5. File Telah Terenkripsi

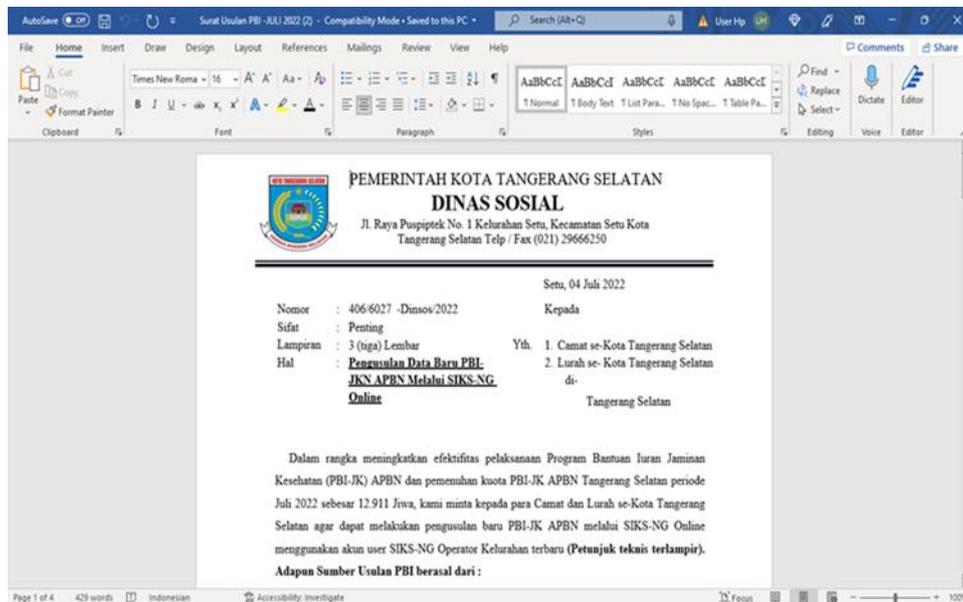
b. Dekripsi File

Pada tampilan layar halaman dekripsi terdapat *form* yang digunakan untuk mendekripsi *file* yang telah terenkripsi. Sebelum melakukan proses dekripsi, *user* harus memilih *file* terlebih dahulu namun bukan memilih *file* asli melainkan memilih *file* yang telah terenkripsi. Lalu kemudian *user* akan diminta memasukkan *password*. Untuk *password* yang digunakan merupakan *password* yang sama pada saat melakukan proses enkripsi minimal 8 karakter.



**Gambar 6.** Halaman Dekripsi

Apabila *user* telah memilih *file* dan memasukkan *password*, maka proses dekripsi dapat berjalan. Apabila proses dekripsi berhasil maka *file* yang telah terdekripsi akan masuk kedalam *database*. Berikut adalah gambaran *file* yang telah terdekripsi.



**Gambar 7.** File Telah Terdekripsi

### 3.2 Pengujian

Pengujian aplikasi adalah sebuah proses yang dilakukan selama penelitian untuk mendapatkan informasi mengenai sistem aplikasi pengamanan *file* di Kelurahan Pakujaya Tangerang Selatan. Proses yang dilakukan untuk melakukan pengujian yaitu proses enkripsi *file* dan dekripsi *file*.

#### a. Pengujian Proses Enkripsi

Pada pengujian proses enkripsi digunakannya *file* asli untuk dilakukannya proses enkripsi. Berikut pengujian dalam proses enkripsi yang dapat dilihat pada tabel:

**Tabel 1.** Pengujian Proses Enkripsi

No.	Nama File Asli	Ukuran File Asli (kb)	Nama File Enkripsi	Ukuran File Enkripsi (KB)	Waktu Enkripsi (Second)
1.	Surat Usulan PBI-Juli 2022	457	Enkrip_Surat_Usulan_PBI_-JULI_2022_(2)	457	9.011

2.	Undangan REMBUK STUNTING TTD WALIKOTA 2022 NEW 7 JULI FIX	125	Enkrip_Undangan_REMBUK_STUNTING_TTD_WALIKOTA_2022_NEW_7_JULI_FIX	125	0.374
3.	Undangan Bimtek 16 Juni 2022	92.6	Enkrip_Undangan_Bimtek_16_Juni_2022	92.6	0.659
4.	Surat Undangan Kesehatan 2	441	Enkrip_Surat_Undangan_Kesahatan_2	441	8.319

b. Pengujian Proses Dekripsi

Pada proses pengujian dekripsi digunakannya *file* yang telah terenkripsi untuk dilakukannya proses dekripsi atau proses pengembalian *file* ke bentuk asli. Berikut proses dekripsi yang dapat dilihat pada tabel:

**Tabel 2.** Pengujian Proses Dekripsi

No.	Nama File	Ukuran File Asli (kb)	Nama File Dekripsi	Ukuran File Dekripsi (KB)	Waktu Dekripsi (Second)
1.	Enkrip_Surat_Usulan_PBI_-JULI_2022_(2)	457	Dekrip_Surat_Usulan_PBI_-JULI_2022_(2)	457	8.911
2.	Enkrip_Undangan_REMBUK_STUNTING_TTD_WALIKOTA_2022_NEW_7_JULI_FIX	125	Dekrip_Undangan_REMBUK_STUNTING_TTD_WALIKOTA_2022_NEW_7_JULI_FIX	125	0.612
3.	Enkrip_Undangan_Bimtek_16_Juni_2022	92.6	Dekrip_Undangan_Bimtek_16_Juni_2022	92.6	0.361
4.	Enkrip_Surat_Undangan_Kesahatan_2	441	Dekrip_Surat_Undangan_Kesahatan_2	441	8.303

c. Hasil Rancangan Pengujian

Berikut adalah hasil dari pengujian program yang telah dilakukan dengan menggunakan *blackbox* dapat dilihat pada tabel:

**Tabel 3.** Hasil Rancangan Pengujian

No.	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian
1.	User dapat mengisi <i>form login</i>	Tampil halaman <i>home</i>	Sesuai harapan
2.	User dapat memilih menu enkripsi	Tampil halaman enkripsi	Sesuai harapan
3.	User dapat mengenkrip <i>file</i> dengan memasukkan <i>password</i> kemudian klik tombol enkripsi	Tampil halaman proses enkripsi	Sesuai harapan

4.	<i>User</i> dapat memilih menu dekripsi	Tampil halaman enkripsi	Sesuai harapan
5.	<i>User</i> dapat mendekrip <i>file</i> dengan menggunakan <i>pass</i> yang sama pada saat enkrip lalu klik tombol dekripsi	Tampil halaman dekripsi	Sesuai harapan
6.	<i>User</i> dapat memilih menu dokumen	Tampil halaman dokumen	Sesuai harapan
7.	<i>User</i> dapat mendownload atau menghapus <i>file</i> yang telah di enkripsi dan di dekripsi	Berhasil <i>download</i> atau berhasil hapus	Sesuai harapan
8.	<i>User</i> dapat memilih menu <i>logout</i>	Kembali ke halaman <i>login</i>	Sesuai harapan

#### 4. KESIMPULAN

Berdasarkan Analisa dan pengujian yang telah dilakukan terhadap permasalahan yang ada pada aplikasi yang telah dibuat maka dapat disimpulkan bahwa aplikasi dapat berjalan dengan baik, aplikasi hanya dapat mengenkripsi dan mendekripsi *file* dengan ekstensi DOCX, XLXS, PDF, dan TXT. Pada aplikasi ini juga apabila melakukan proses enkripsi dan dekripsi tidak akan mengubah ukuran *file* sehingga ukuran *file* masih seperti ukuran asli.

Pada peneliiian selanjutnya diharapkan dapat mengembangkan aplikasi sehingga tidak hanya dapat menggunakan *file* dengan ekstensi DOCX, XLXS, PDF, dan TXT tetapi dapat mengamankan *file* dengan berbagai macam ekstensi seperti gambar, audio, serta video.

#### DAFTAR PUSTAKA

- [1] Busran and J. W. Putra, "Analisa Komputasi Algoritma Des Dengan RC4 Untuk Keamanan Data," *Jurnal Teknoif ITP*, vol. 9, no. 1, pp. 20-23, 2021.
- [2] R. Maulana and R. M. Simanjorang, "Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *JNKTI: Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 4, no. 6, pp. 377-383, 2021.
- [3] A. Yuliandesi, D. Rukmana Sitompul, A. P. Ajf, and M. A. Hasan, "Implementasi Algoritma MD5 dan RC4 Untuk Keamanan Data File," *Jurnal Teknik Informatika*, pp. 1-6, 2020.
- [4] S. A. Rudiyanto, "Teks Pada Aplikasi Chatting Berbasis Android Dengan Metode Vigenere Cipher Pada Smk Negeri 7 Kota Chatting Berbasis Android Dengan Metode Vigenere Cipher Pada Smk Negeri 7," *SKANIKA*, vol. 1, no. 2, pp. 758–765, 2018.
- [5] H. Kusniyati, S. Diansyah, and R. Yusuf, "Penerapan Algoritma Rivert Code 4 (RC4) Pada Aplikasi Kriptografi Dokumen," *Jurnal PETIR*, vol. 11, no. 1, pp. 38-47, 2018.
- [6] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, and I. Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, pp. 114-119, 2020.
- [7] Rista, A. S. Sitio, "Implementasi Keamanan Data Keuangan di SMK Swasta Musda Perbaungan Menggunakan Metode RC4," vol. 3, no. 3, pp. 60–66, 2021.
- [8] K. Kirman, "Implementasi Algoritma Rc4 Untuk Proteksi File Mp3," *Jurnal Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018.
- [9] M. Hayaty and M. D. Putra, "Enkripsi Dan Dekripsi Gambar Dengan Menggunakan Perpaduan Algoritma Base64 dan RC4," *Core It*, vol. 5, pp. 1–6, 2018.
- [10] Perancangan Basis Data.