

# Implementasi Algoritma One Time Pad Untuk Proteksi File Data Pribadi Pada Aplikasi Berbasis Web

Implementation of One Time Pad Algorithm to Protect Personal Data File on Web Based Applications

**Lalang Erawan<sup>1\*</sup>, Suharnawi<sup>2</sup>**

<sup>1,2</sup> Program Studi Sistem Informasi

<sup>1,2</sup> Fakultas Ilmu Komputer, Universitas Dian Nuswantoro

Jl. Nakula I No. 5-11, Semarang, Jawa Tengah 50131, Telp. 0243517261

Email: <sup>1\*</sup>lalang.erawan@dsn.dinus.ac.id, <sup>2</sup>suharnawi@dsn.dinus.ac.id

## **Abstrak**

*Penelitian bertujuan untuk menerapkan algoritma kriptografi One Time Pad pada sebuah aplikasi berbasis web yang berfungsi untuk mengamankan file data pribadi pengguna internet ketika akan digunakan di media internet untuk ditransmisikan atau disimpan dalam cloud storage. Algoritma ini terbukti unbrekable karena password untuk enkripsi dan dekripsi hanya digunakan sekali dan panjangnya sama dengan panjang pesan yang dienkripsi. Dengan pengamanan ini, file data pribadi pengguna internet menjadi lebih kuat terhadap serangan penyalahgunaan data yang dapat menimbulkan kerugian bagi mereka. Jenis file yang digunakan untuk menyimpan data pribadi dalam penelitian ini dibatasi 3 jenis yaitu file teks, pdf, dan word karena jenis tersebutlah yang paling banyak digunakan orang untuk bertukar informasi. Data penelitian adalah sejumlah file dengan ukuran maksimal 100 KB dan berjenis dokumen pengolah kata (doc), portable document (pdf), dan teks (txt). Metode pengembangan sistem yang digunakan adalah rekayasa web yang terdiri dari langkah komunikasi, perencanaan, pemodelan, konstruksi, dan penyebaran. Alat pemodelan menggunakan diagram UML. Rancangan aplikasi diuji dengan metode blackbox, dan uji kecepatan enkripsi dan dekripsi. Hasil pengujian kecepatan menunjukkan kelayakan kecepatan aplikasi pada media web. Penelitian menghasilkan rancangan aplikasi web beserta prototypenya. Aplikasi ini akan dapat digunakan oleh para pengguna internet secara bebas untuk mengamankan file-file data pribadi yang akan mereka gunakan di internet. Meskipun file data pribadi sudah diproteksi, sebaiknya password yang digunakan untuk memproteksi dan membuka proteksi dikirim melalui media komunikasi lain, misalnya saluran telepon, dengan tujuan untuk mengurangi potensi penyadapan data.*

**Kata kunci:** aplikasi web, keamanan data, kriptografi klasik, one time pad.

## **Abstract**

*The research aims to apply the One Time Pad cryptographic algorithm in a web-based application that serves to secure the personal data files of internet users when it will be used on internet media to be transmitted or stored in cloud storage. This algorithm is proven to be unbrekable because the passwords for encryption and decryption are only used once and the length is the same as the length of the message encrypted. With this security, the personal data files of internet users become stronger against data abuse attacks that can cause harm to them. The file types used to store personal data in this study are limited to 3 types, namely text, pdf, and word files because they are the type most used by people to exchange information. The research data are a number of files with a maximum size of 100 KB and types of word processing documents (doc), portable document (pdf), and text (txt). The system development method used is web engineering which consists of steps in communication, planning, modeling,*

construction, and deployment. The modeling tool uses UML diagrams. The design of the application is tested by the blackbox method, and the encryption and decryption speed test. The results of speed testing show the appropriateness of the speed of application on web media. The research resulted in the design of web applications and their prototypes. This application will be used by internet users freely to secure personal data files that they will use on the internet. Although personal data files have been protected, passwords that are used to protect and open protection should sent through other communication media, such as telephone lines, to reduce the potential for data tapping.

**Keywords:** web application, data security, classic cryptography, one time pad.

## 1. PENDAHULUAN

Penelitian-penelitian sebelumnya telah dilakukan dengan menggunakan berbagai metode kriptografi dan atau steganografi untuk membangun aplikasi keamanan data. Sebagian besar penelitian menggunakan basis desktop sebagai platform aplikasinya. Aplikasi dengan basis web dilakukan pada satu penelitian oleh Agustina dan kawan-kawan dengan metode kriptografi RSA dan jenis file yang digunakan office dan teks [1]. File office yang digunakan meliputi file doc, docx, xls, ppt, dan pptx. Penelitian ini belum mempertimbangkan faktor kecepatan aplikasi dalam melakukan proses enkripsi dan dekripsi pesan dalam media web. Sementara faktor kecepatan merupakan salah satu faktor kritis keberhasilan aplikasi di media web. Selain itu, penelitian tersebut tidak menyertakan jenis file pdf yang sering digunakan untuk bertukar informasi.

Penelitian ini bertujuan untuk membangun sebuah aplikasi web untuk melindungi file data pribadi pengguna internet yang mempertimbangkan faktor kecepatan proses *chipering* dan menambahkan satu jenis file yang dapat digunakan yaitu jenis file pdf yang sering digunakan untuk saling bertukar informasi. Penyertaan faktor kecepatan aplikasi diharapkan meningkatkan kelayakan aplikasi sebagai aplikasi yang berbasis web dan meningkatkan kebermanfaatannya dengan menambahkan satu jenis file dalam penggunaannya.

Penelitian menggunakan teknik kriptografi untuk mengamankan datanya. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Pesan dapat berbentuk data atau informasi yang dikirim melalui saluran telekomunikasi atau yang disimpan didalam media rekam. Pesan yang tersimpan dapat berupa gambar, suara, video, atau berkas digital lainnya. Kriptografi terdiri dari beberapa elemen yang membentuk sebuah sistem yang disebut sistem kriptografi yang terdiri dari algoritma kriptografi, plainteks, chiperteks, dan kunci. Sesuai definisinya, kriptografi bertujuan untuk memberikan layanan keamanan yang juga disebut aspek-aspek keamanan yang terdiri dari kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. Berdasarkan sejarahnya, kriptografi dibagi menjadi kriptografi klasik dan modern. Berdasarkan kunci enkripsi dan dekripsi, kriptografi dibedakan menjadi kriptografi kunci simetri dan kunci asimetri. Kriptografi kunci simetri menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi. Sedangkan kriptografi kunci asimetri menggunakan kunci yang berbeda. Semua kriptografi klasik merupakan kriptografi kunci simetris. Sedangkan kriptografi modern sebagian merupakan kriptografi kunci simetris seperti DES dan AES. Pada dasarnya kriptografi kunci simetri beroperasi dalam salah satu dari dua jenis operasi, yaitu mode blok dan aliran. Mode blok beroperasi terhadap satu blok data setiap kali melakukan enkripsi dan dekripsi data. Mode aliran mengenkripsi dan mendekripsi 1 bit atau byte data setiap kalinya.

*One Time Pad* termasuk kategori algoritma kriptografi (*chiper*) klasik kunci simetris. Satu-satunya chiper yang tidak dapat dipecahkan. Rumus enkripsi algoritma *One Time Pad* dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci dengan persamaannya  $c_i = (p_i + k_i) \bmod 26$ , dimana  $c_i$  adalah karakter chiperteks ke- $i$ ,  $p_i$  karakter plainteks ke- $i$ , dan  $k_i$  karakter kunci ke- $i$ . Sedangkan rumus dekripsi *One Time Pad* adalah  $p_i = (c_i - k_i) \bmod 26$  [2].

Dalam penelitian ini metode pengembangan sistem yang digunakan adalah metode rekayasa web (*web engineering*) yang terdiri dari 5 tahap yaitu komunikasi (*communication*), perencanaan (*planning*), pemodelan (*modeling*), konstruksi (*construction*), dan penyebaran (*deployment*) [3].

## 2. METODE PENELITIAN

Jenis file yang dapat digunakan dalam aplikasi dibatasi hanya 3 jenis, yaitu file pengolah kata (*doc*), file dokumen portable (*pdf*), dan file teks (*txt*). Ukuran file juga dibatasi sampai dengan 100 KB mengingat aplikasi berjalan pada media jaringan internet yang memiliki keterbatasan saluran transmisi data (*bandwidth*). Oleh karena itu dalam penelitian ini data yang digunakan berupa 3 jenis file seperti yang disebutkan sebelumnya. Masing-masing jenis file berjumlah 3 buah, satu buah berukuran dibawah 100 KB, dan satu buah berukuran 100 KB keatas. File-file ini digunakan terutama untuk melakukan pengujian terhadap fungsi-fungsi utama aplikasi yaitu fungsi enkripsi untuk mengamankan file data pribadi dengan mengacaknya menggunakan algoritma One Time Pad dan fungsi dekripsi untuk mengembalikan pesan acak ke bentuknya semula.

Metode pengembangan aplikasi yang digunakan adalah metode rekayasa web (*web engineering*) yang terdiri dari langkah-langkah sebagai berikut:

### 1. Komunikasi

Pada langkah ini dilakukan pengumpulan data dan informasi yang diperlukan dalam penelitian termasuk jenis-jenis file yang akan digunakan untuk melakukan pengujian aplikasi.

### 2. Perencanaan

Pada langkah ini pekerjaan dan jadwal pembangunan aplikasi diidentifikasi dan disusun.

### 3. Pemodelan

Setelah pekerjaan dan jadwal pelaksanaan disusun, langkah selanjutnya adalah membuat model dari aspek-aspek aplikasi yang meliputi spesifikasi persyaratan fungsional, modul-modul program, database, dan arsitektur aplikasi.

### 4. Konstruksi

Model-model yang dihasilkan pada langkah sebelumnya kemudian dijadikan dasar pembuatan kode-kode program dari aplikasi. Setelah kode program terbentuk maka dilakukan pengujian terhadap aplikasi menggunakan metode *blackbox* untuk memastikan fungsional aplikasi bekerja sesuai rancangan dan pengujian kecepatan proses enkripsi dan dekripsi aplikasi.

### 5. Penyebaran

Pada langkah ini melibatkan calon pengguna aplikasi untuk mencoba aplikasi dan memberikan umpan balik. Perbaikan terhadap aplikasi akan dilakukan berdasarkan umpan balik yang diberikan calon pengguna. Proses perbaikan akan terus dilakukan sampai calon pengguna dapat menerima versi perbaikan aplikasi terakhir.

Setelah dikonstruksi aplikasi akan diuji menggunakan beberapa metode pengujian berikut ini:

#### 1. *Black Box Testing*

Aplikasi akan diuji menggunakan metode *black box*. Metode ini akan menguji aplikasi terhadap berbagai input yang mungkin terhadap fungsi-fungsi aplikasi untuk mengetahui apakah keluaran proses seperti yang sudah dispesifikasikan. Metode pengujian ini tidak memperhatikan

struktur internal aplikasi. Pengujian akan menggunakan spesifikasi aplikasi yang telah disusun pada awal pengembangan sistem.

## 2. Page Load Times Testing

Faktor waktu muat halaman (*page load times*) menentukan kecepatan pemuatan halaman (*page speed*) untuk aplikasi berbasis web. Faktor ini merupakan salah satu ukuran keberhasilan aplikasi. Berdasarkan laporan hasil studi google terhadap kecepatan aplikasi web di perangkat genggam [14], meskipun platform desktop masih menjadi platform utama tetapi saat ini lebih dari setengah pengguna internet menggunakan perangkat bergerak mereka untuk mengakses layanan web. Situs-situs dengan kecepatan muat halaman antara 1 sampai dengan 3 detik berpotensi ditinggal pergi pengguna sebesar 32%, 1 sampai dengan 5 detik 90%, 1 sampai dengan 6 detik 106%, dan 1 sampai dengan 10 detik 123%.

Berdasarkan laporan hasil penelitian google tersebut, dalam penelitian ini aspek kecepatan aplikasi dijadikan salah satu faktor uji aplikasi untuk memastikan kelayakan penggunaan aplikasi dari sisi waktu. Waktu muat halaman yang digunakan dalam penelitian ini ditentukan 5 detik. Alat yang digunakan untuk menguji kecepatan aplikasi adalah aplikasi *App.telemetry Page Speed Monitor*.

## 3. HASIL DAN PEMBAHASAN

Data yang digunakan dalam penelitian berupa file-file data yang berjenis pengolah kata (*doc*), dokumen portable (*pdf*), dan teks (*txt*). File-file ini digunakan untuk menguji aplikasi. Keseluruhan jumlah file yang digunakan adalah 9 buah file dengan rincian sebagai berikut:

Tabel 1. Tabel File Data Untuk Pengujian

No	Nama File	Jenis	Ukuran (KB)
1	abstrak.doc	docx	17
2	Laporan keuangan.doc	docx	80
3	Arsitektur Web.doc	docx	182
4	Nilai Tugas.pdf	pdf	22
5	Algoritma klasik.pdf	pdf	59
6	Diagram Fishbone.pdf	pdf	132
7	kunci.txt	txt	2
8	e-bisnis.txt	txt	63
9	konfigurasi sistem.txt	txt	106

Proses enkripsi dengan algoritma *One Time Pad* memerlukan kunci sepanjang file plainteks. Untuk menghasilkan kunci ini menggunakan password yang dimasukkan oleh pengguna. Teknik pembangkitan kunci yang diperlukan ini menggunakan teknik seperti yang diusulkan oleh Pratama [5]. Metode ini cukup sederhana dalam implementasinya tetapi tetap menghasilkan deretan kunci yang diperlukan dengan baik. Metode pembangkit kunci ini menggunakan karakter 'A' sampai dengan 'Z'. Langkah-langkah pembangkitan kunci sebagai berikut:

1. Karakter terakhir dari kunci dijumlahkan dengan n-1 karakter sebelumnya (n adalah panjang kunci asli), kemudian jumlah tersebut dikenakan modulo 26.
2. Hasil modulo merupakan karakter baru yang kemudian digabungkan dengan kunci sebelumnya menjadi kunci baru.
3. Proses kembali mengulang langkah pertama sampai kunci sepanjang plaintext.

Berdasarkan langkah-langkah diatas, diperoleh rumus sebagai berikut untuk menghasilkan kunci ke-i:

$$k_i = (k_{i-n} + k_{i-1}) \bmod 26 \tag{1}$$

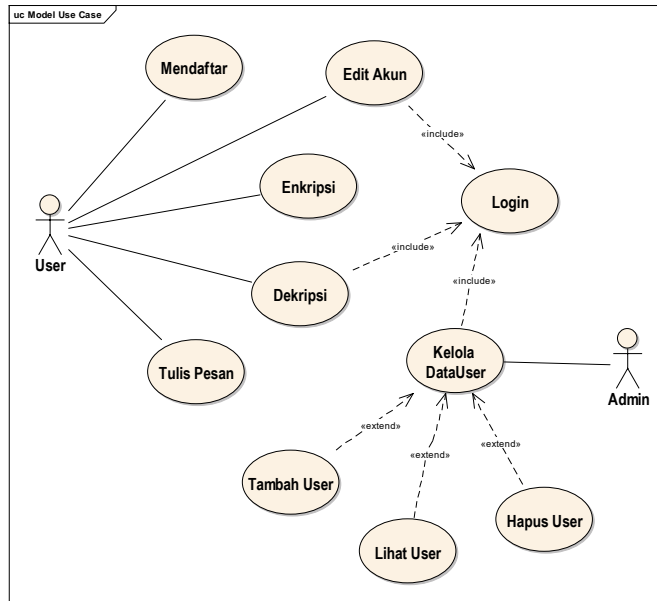
dimana:

$i = n+1, n+2, \dots$

$k_i$  = karakter kunci ke- $i$  ( $A=0, B=1, \dots$ )

$n$  = panjang kunci asli

Persyaratan fungsional aplikasi dimodelkan menggunakan diagram use case disertai dengan skenarionya. Diagram use case akan menggambarkan interaksi antara pengguna dengan sistem. Rincian interaksi dijelaskan dengan skenario use case.



Gambar 1. Diagram Use Case Fungsional Aplikasi

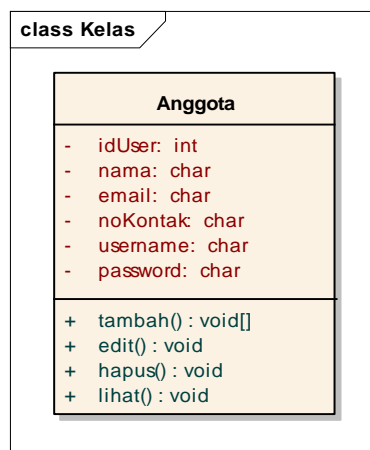
Rincian setiap use case dalam diagram use case diatas dijelaskan lebih lanjut menggunakan skenario use case. Berikut ini skenario use case untuk enkripsi dan dekripsi:

Nama Use Case	Enkripsi
Deskripsi	Pengguna diminta untuk memasukkan <i>file plaintext</i> yang akan diacak dan password untuk mengacak pesan dalam <i>file plaintext</i> . Hasil proses berupa <i>file ciphertext</i> yang siap diunduh dan password maupun <i>file plaintext</i> dan <i>ciphertext</i> tidak disimpan kedalam database untuk alasan keamanan. Pengguna dapat mengirimkan password pembuka <i>file ciphertext</i> melalui email atau media lain yang aman ke penerima pesan.
Aktor	Pengguna
Prakondisi	-
Langkah-langkah	
Aktor	Sistem
1. Memilih Menu Enkripsi 3. Memasukkan <i>file plaintext</i> dan password	2. Menampilkan Form Enkripsi 4. Membangkitkan pasword sepanjang <i>file plaintext</i> 5. Mengacak pesan dalam <i>file plaintext</i> dengan

	password yang dibangkitkan Menulis hasil pengacakan ke <i>file</i> Membuat link untuk mengunduh <i>file</i>
Postkondisi	Terbentuk <i>file chipertext</i> yang siap diunduh

Nama Use Case	Dekripsi
Deskripsi	Pengguna diminta untuk memasukkan <i>file chipertext</i> yang akan dibuka berikut password untuk membukanya. Hasil proses berupa <i>file plaintext</i> yang siap diunduh.
Aktor	Pengguna
Prakondisi	<i>File chipertext</i> sudah dibuat dan pengguna sudah melakukan login ke aplikasi
Langkah-langkah	
Aktor	Sistem
1. Memilih Menu Dekripsi 3. Memasukkan <i>file chipertext</i> dan password	2. Menampilkan Form Dekripsi 4. Membangkitkan pasword sepanjang <i>file chipertext</i> 5. Mengembalikan pesan kedalam bentuk awal sebelum diacak dengan password yang dibangkitkan 6. Menulis hasil dekripsi menjadi <i>file plaintext</i> . 7. Membuat Link untuk mengunduh <i>file plaintext</i>
Postkondisi	Link untuk mengunduh <i>file plaintext</i> terbentuk

Database yang digunakan dalam aplikasi meminimalkan informasi yang perlu disimpan untuk meningkatkan keamanan aplikasi dari peretasan. Maka file-file pengguna maupun hasil enkripsi dan dekripsi tidak akan disimpan kedalam database. Demikian juga halnya dengan password yang digunakan untuk proses enkripsi. Dengan demikian aplikasi ini hanya menggunakan satu tabel yang digunakan untuk menyimpan data keanggotaan. Data ini perlu disimpan karena fitur dekripsi tidak dapat diakses kecuali pengguna memiliki akun aplikasi. Hal ini dilakukan agar fitur dekripsi tidak mudah untuk disalahgunakan. Adapun rancangan database aplikasi sebagai berikut:



Gambar 2. Diagram Kelas Rancangan Database Aplikasi

Selesai dikonstruksi, aplikasi kemudian dikenakan beberapa pengujian untuk memastikan aplikasi tidak mengandung kesalahan dan sesuai dengan rancangan.

Pengujian blackbox akan menguji kesesuaian aplikasi dengan persyaratan fungsional yang dirancang dengan diagram use case. Setiap skenario pada use case diuji untuk memastikan keluaran setiap proses telah sesuai rancangan. Berikut ini daftar hasil pengujianya:

Tabel 2. Hasil Pengujian Metode Black Box

No	Skenario	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Pengguna bermaksud mengamankan file data (enkripsi) dengan masukan berupa file data dan password untuk enkripsi pada form <i>Pasang Pengaman</i>	Link untuk mengunduh file hasil enkripsi terbentuk dan file hasil dapat diunduh	Link terbentuk dan file hasil dapat diunduh	Valid
2	Sebelum login, pengguna bermaksud membuka pengaman pada suatu file pada form <i>Buka Pengaman</i> dengan masukan file hasil enkripsi dan password yang digunakan untuk enkripsi	Muncul pesan peringatan bahwa pengguna belum melakukan login	Muncul pesan peringatan belum login	Valid
3	Setelah login, pengguna bermaksud membuka pengaman pada suatu file pada form <i>Buka Pengaman</i> dengan masukan file hasil enkripsi dan password yang digunakan untuk enkripsi	Link untuk mengunduh hasil proses akan terbentuk dan file hasil dapat diunduh	Link terbentuk dan file hasil dapat diunduh	Valid

Hasil pengujian black box terhadap fungsional aplikasi menghasilkan kesimpulan bahwa fungsi-fungsi aplikasi telah berjalan dengan baik dan benar sesuai rancangan.

Pengujian berikutnya adalah menguji kemampuan aplikasi dalam mengenkripsi dan mendekripsi jenis-jenis file data yang sudah ditetapkan (doc, pdf, txt). Dalam pengujian ini juga akan diperoleh informasi tentang kecepatan proses enkripsi dan dekripsi terhadap berbagai ukuran file data. Alat yang digunakan untuk mengukur kecepatan adalah *App.telemetry Page Speed Monitor*. Berikut ini tabel hasil pengujianya:

Tabel 3. Pengujian Kecepatan Menggunakan Jenis File Data Berbeda

No	File Uji	Ukuran File	Enkripsi/Dekripsi	Kecepatan (detik)
1	abstrak.doc	17 KB	berhasil/berhasil	1,3/1,4
2	Laporan keuangan.doc	80 KB	berhasil/berhasil	4,6/4,8
3	Arsitektur Web.doc	182 KB	gagal/gagal	-/-
4	Nilai Tugas.pdf	22 KB	berhasil/berhasil	2,13/1,53
5	Algoritma klasik.pdf	59 KB	berhasil/berhasil	3,47/3,47
6	Diagram Fishbone.pdf	132 KB	gagal/gagal	-/-
7	kunci.txt	2 KB	berhasil/berhasil	0,44/0,42
8	e-bisnis.txt	63 KB	berhasil/berhasil	3,53/
9	konfigurasi sistem.txt	106 KB	gagal/gagal	-/-

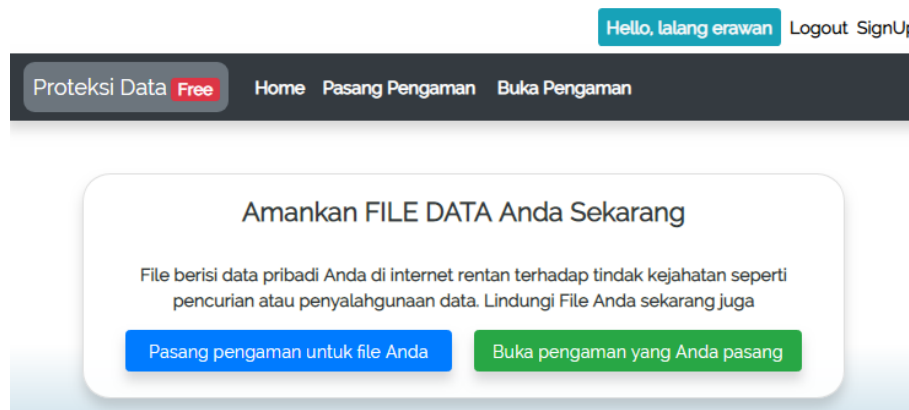
Seperti rancangan yang telah dibuat, file-file *doc*, *pdf*, dan *txt* dengan ukuran 100 KB kebawah telah berhasil dienkripsi maupun didekripsi dengan kecepatan dibawah 5 detik. Sementara file yang berukuran lebih besar dari 100 KB tidak dapat dienkripsi dan didekripsi.

Selain memperoleh hasil tingkat kecepatan proses enkripsi dan dekripsi setiap file, diperoleh juga hasil yang memastikan bahwa tindakan mengenkripsi file-file tersebut tidak akan terdeteksi secara kasat mata karena ukuran file sebelum dan setelah dienkripsi tidak berubah sebagai berikut:

Tabel 4. Hasil Uji Menunjukkan Ukuran File Uji Tidak Berubah

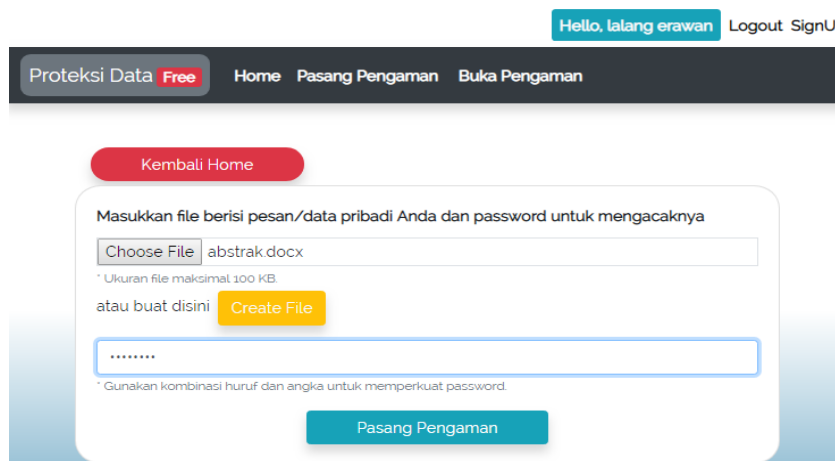
No	File Uji	Ukuran File Sebelum Enkripsi	Ukuran File Setelah Enkripsi
1	abstrak.doc	17 KB	17 KB
2	Laporan keuangan.doc	80 KB	80 KB
4	Nilai Tugas.pdf	22 KB	22 KB
5	Algoritma klasik.pdf	59 KB	59 KB
7	kunci.txt	2 KB	2 KB
8	e-bisnis.txt	63 KB	63 KB

Proses pengembangan aplikasi melalui beberapa inkremen atau iterasi. Setiap inkremen menghasilkan versi aplikasi tertentu. Setelah beberapa kali perbaikan berdasarkan umpan balik yang diberikan calon pengguna, maka dihasilkan aplikasi yang sesuai dengan harapan calon pengguna. Adapun versi terakhir aplikasi yang sesuai harapan pengguna adalah sebagai berikut:



Gambar 3. Halaman awal aplikasi

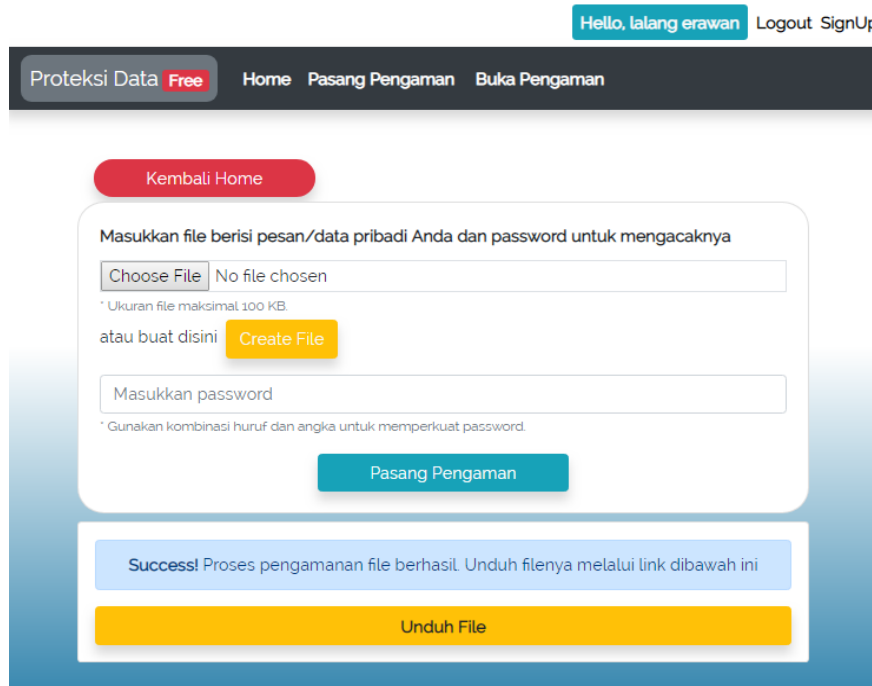
Pada halaman pertama aplikasi pengguna dapat memilih menu ‘Pasang Pengaman’ atau tombol “Pasang pengaman untuk file Anda” untuk mengenkripsi file data yang akan menampilkan sebuah form:



Gambar 4. Form untuk mengenkripsi file data pribadi pengguna

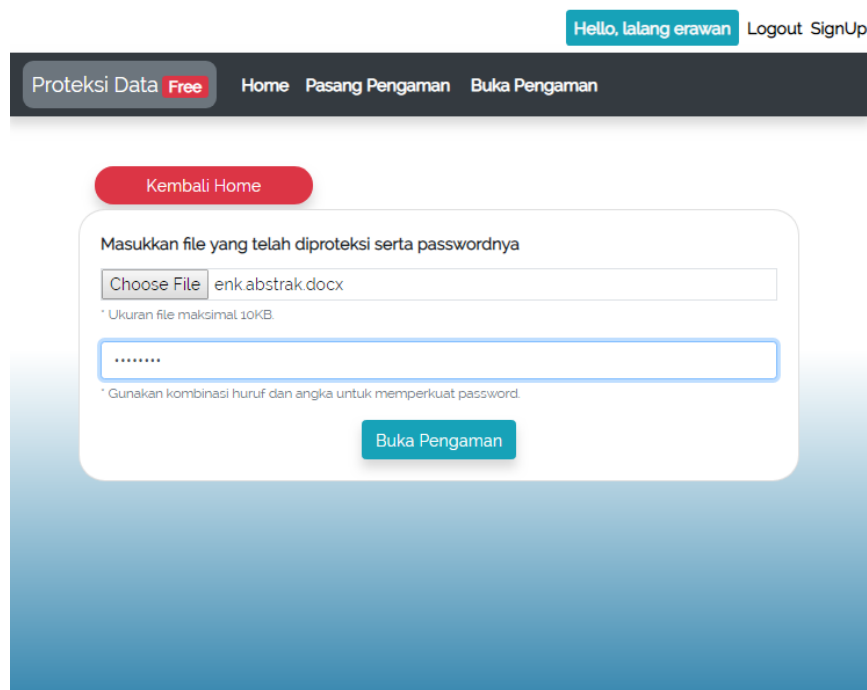


Pada isian pertama form proteksi diatas pilih file berisi data pribadi yang akan diproteksi, pada gambar diatas dipilih file berjenis doc yaitu 'abstrak.docx'. Isian kedua adalah password yang akan digunakan untuk memproteksi. Tekan tombol 'Pasang Pengaman' untuk memulai proses proteksi. Setelah proses selesai maka pengguna akan memperoleh sebuah link untuk mengunduh file yang telah dienkripsi:



Gambar 5. Link untuk mengunduh file hasil enkripsi

Untuk membuka proteksi atau menjalankan dekripsi terhadap file hasil enkripsi pengguna harus login terlebih dahulu baru bisa memilih menu 'Bongkar' yang akan menampilkan form dekripsi:



Gambar 6. Form untuk proses dekripsi

Masukkan file hasil enkripsi sebelumnya kedalam isian pertama kemudian pada isian kedua masukkan password yang tadi digunakan untuk mengenkripsi. Setelah itu klik tombol 'Buka Pengaman' maka akan tampil link untuk mengunduh file hasil dekripsi berisi data yang sudah tidak teracak lagi.

Gambar 7. Link unduh hasil dekripsi

#### 4. KESIMPULAN

Aplikasi web pengaman data pribadi ini menggunakan chiper yang terbukti *unbreakable* sehubungan dengan panjangnya kunci dan password sekali pakai. Dari sisi teknik enkripsi yang digunakan, kekuatan dan keamanan proteksi terhadap file data pribadi tidak diragukan lagi. Untuk memperkuat keamanan data, file data pengguna, dan password yang digunakan untuk proses enkripsi tidak disimpan kedalam database sehingga memperkecil resiko terbongkarnya file *chiper* hasil enkripsi dari pihak yang tidak bertanggung jawab. File data yang telah melalui proses enkripsi dalam aplikasi ini tidak akan menimbulkan kecurigaan bahwa telah diamankan karena ukuran file asli dan file hasil enkripsi tidak berbeda. Pengujian dengan metode blackbox memastikan aplikasi telah berjalan sesuai spesifikasinya. Agar keamanan data pribadi lebih terjamin lagi, pengiriman password yang digunakan kepada pihak penerima sebaiknya menggunakan media telekomunikasi lain, misalnya lewat saluran telepon.

#### 5. SARAN

Aplikasi yang dihasilkan dari penelitian ini masih dapat dikembangkan lebih lanjut untuk lebih meningkatkan keamanan data pengguna aplikasi. Teknik pembangkitan password yang digunakan dalam penelitian menggunakan cara sederhana dan mengandung beberapa kelemahan [9]. Teknik pembangkitan password yang digunakan dapat dikaji lebih jauh untuk menggunakan teknik yang lebih kuat lagi, misalnya menggunakan model Blum Blum Shub Generator yang lebih sulit diprediksi oleh kriptanalis.

**DAFTAR PUSTAKA**

- [1] Agustina, A.N., Aryanti, Nasron, (2017), Pengamanan Dokumen Menggunakan Metode RSA (Rivest Shamir Adleman) Berbasis Web, Konferensi Nasional SENDI, 3, pp. 14-19
- [2] Munir, R., (2009), Kriptografi, Informatika, Bandung, pp. 2-96
- [3] Pressman, R.S., Lowe, D. (2009), Web Engineering-A Practitioner's Approach, McGraw-Hill, New York, pp. 24-45
- [4] Pratama, A., (2010), Pembangkit kunci untuk Chiper One-time Pad, Jurusan Teknik Informatika Sekolah Teknik Elektro dan Informatika ITB, Bandung
- [5] Thinkwithgoogle.com (2017) Find Out How You Stack Up to New Industry Benchmarks for Mobile Page SpeedGoogle. [online], <https://think.storage.googleapis.com/docs/mobile-page-speed-new-industry-benchmarks.pdf>, tanggal akses: 08 Nopember 2018