Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 588-597
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Teknik Keamanan *File* Teks Menggunakan Kriptografi Dengan Algoritma *One Time Pad* Cipher

Muhammad Reza Fahlevi [1], Dini Ridha Dwiki Putri [2], Rahmad Doni [3]
[1] Rekayasa Sistem Komputer, Universitas Potensi Utama
[2,3] Rekayasa Perangkat Lunak, Universitas Potensi Utama
ezafahlevi72@gmail.com, putrydiny11@gmail.com, rahmaddoni113@gmail.com

Abstract

In maintaining a data that needs to be considered in system security is the authentication process. This process is carried out to ensure users who access data or information on the system are authorized users. There are several methods to authenticate, one of them using data encryption (cryptographic) techniques. Cryptography is applied to data or information by encoding or organizing the data needed only by those who have the key to which the data or information can be accessed. This research will implement the One Time Pad (OTP) algorithm to encode the data and information used. Data or information transferred in the application will form a ciphertext so that users will get a key to access the data or information. The making of this application is expected to guarantee the confidentiality and security of data properly, where the party that can access the original data or information is only the party that has the key.

Keywords : *Cryptography , Text File, One Time Pad Algorithm*

Abstrak

Dalam menjaga suatu data yang perlu diperhatikan dalam keamanan sistem adalah proses autentikasi. Proses ini dilakukan untuk memastikan pengguna yang mengakses data atau informasi pada sistem tersebut adalah pengguna yang memiliki wewenang. Ada beberapa metode untuk melakukan autentikasi, salah satunya dengan menggunakan teknik penyandian data (kriptografi). Kriptografi banyak di pakai pada data atau informasi dengan menyembunyikan atau mengakses data yang diperlukan hanya bagi yang memiliki akses kunci yang dapat diakses data atau informasi tersebut. Penelitian ini akan mengimplementasikan algoritma One Time Pad (OTP) untuk melakukan penyandian terhadap data dan informasi yang digunakan. Data atau informasi yang dipindahkan dalam aplikasi akan membentuk ciphertext sehingga pengguna akan mendapatkan kunci untuk mengakses data atau informasi tersebut. Pembuatan perangkat lunak (aplikasi) ini diharapkan dapat menjamin integritas suatu kerahasiaan dan keamanan data atau informasi dengan baik, dimana user yang dapat mengakses suatu data atau informasi yang asli dari sumbernya yang memiliki kunci.

Kata kunci *: Kriptografi, File Teks, algoritma One Time Pad.*

1. PENDAHULUAN

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi saat ini. Semakin pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya suatu teknik yang baru yang disalahgunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Ironisnya, teknik yang digunakan

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 588-597
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

untuk mengancam keamanan data selalu setingkat lebih maju. Kriptografi sendiri sudah digunakan sejak zaman dahulu hingga saat ini dimana perkembangan teknologi informasi begitu pesat. Dari Beberapa metode algoritma kriptografi banyak yang diciptakan dengan perhitungan yang sangat rumit dengan tujuan agar pesan (data) yang di amankan tidak mudah untuk dipecahkan. Dari penelitian ini juga akan mengimplementasikan metode kriptografi yaitu *One Time Pad* (OTP), dimana metode ini menggunakan setiap kunci (*key*) yang sama dalam proses penyandian(enkripsi) maupun dekripsi. Dimana metode ini sipengirim dan sipenerima menyetujui suatu kunci tertentu sebelum terjadi berkomunikasi diantara keduanya. Ruang cakupan yang akan dibahas pada penelitian ini adalah teknik keamanan file teks menggunakan kriptografi dengan algoritma OTP, dimana pesan dan informasi berupa *file* dengan format teks. Dengan menerapkan algoritma OTP pada pengamanan *file* teks, sehingga keamanan data maupun informasi dapat terjaga dengan baik.

Dalam komunikasi data ada sebuah metode keamanan data yang sering kita kenal dengan nama kriptografi. Kriptografi adalah satu dari sekian metode keamanan data yang selalu diterapkan untuk menjamin suatu kerahasiaan, keaslian, juga keaslian pengiriman. Algoritma ini bertujuan agar suatu data yang bersifat rahasia yang dikirim melalui media tidak dapat diketahui atau dicuri oleh orang yang tidak berkepentingan atau yang tidak berhak menerimanya. Metode kriptografi digunakan untuk mengamankan data ada bermacam-macam tingkat keamanannya. Setiap metode kriptografi mempunyai keunggulan dan kelemahannya masing-masing. Namun, yang sering terjadi permasalahan adalah memilih algoritma kriptografi yang tepat. Dalam alur proses komunikasi, walaupun data yang sudah dienkripsi kemungkinan data tersebut dapat diketahui oleh orang yang tidak berkepentingan. Salah satu kejadian tersebut adalah orang-orang tersebut menyadap media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi. Hal ini adalah merupakan masalah yang utama bagi setiap pengguna dalam mengamankan data-datanya yang penting. Maka untuk menghindari hal-hal tersebut perlu pengamanan data, diantaranya dengan menggunakan kriptografi baik itu dengan sifat klasik maupun modern.

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan oleh penulis dengan metode penelitian deskriptif atau biasa dikenal dengan metode penelitian analitis. Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, survei, studi kepustakaan terhadap masalah-masalah yang berhubungan dengan keamanan data, teknik pengujian terhadap objek penelitian yang telah ada. Metode penelitian deskriptif dipilih penulis dikarenakan pemecahan masalah yang aktual yaitu masalah yang berkembang pada bidang artifisial *intelligence* yang saat ini sedang berkembang. Menggunkan metode deskriptif, dengan data

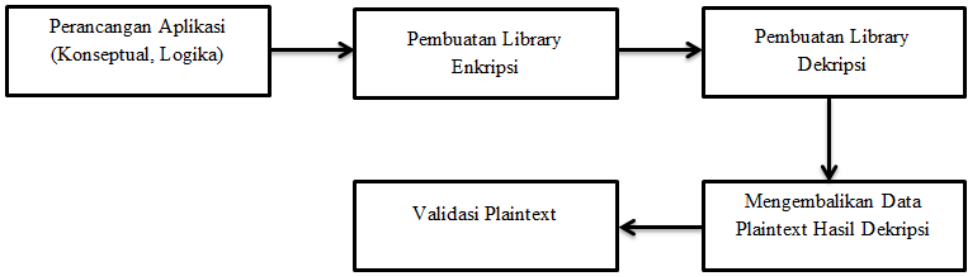
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 588-597
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

yang telah penulis kumpulkan kemudian disusun, dijelaskan, dianalisis, dan kemudian diimplementasikan dalam sebuah perangkat lunak (aplikasi).

Dalam melaksanakan penelitian ini terdapat beberapa cara atau teknik yang penulis gunakan untuk menyelesaikan suatu masalah diantaranya diperoleh dengan cara sebagai berikut:

2.1. Alur Rancangan

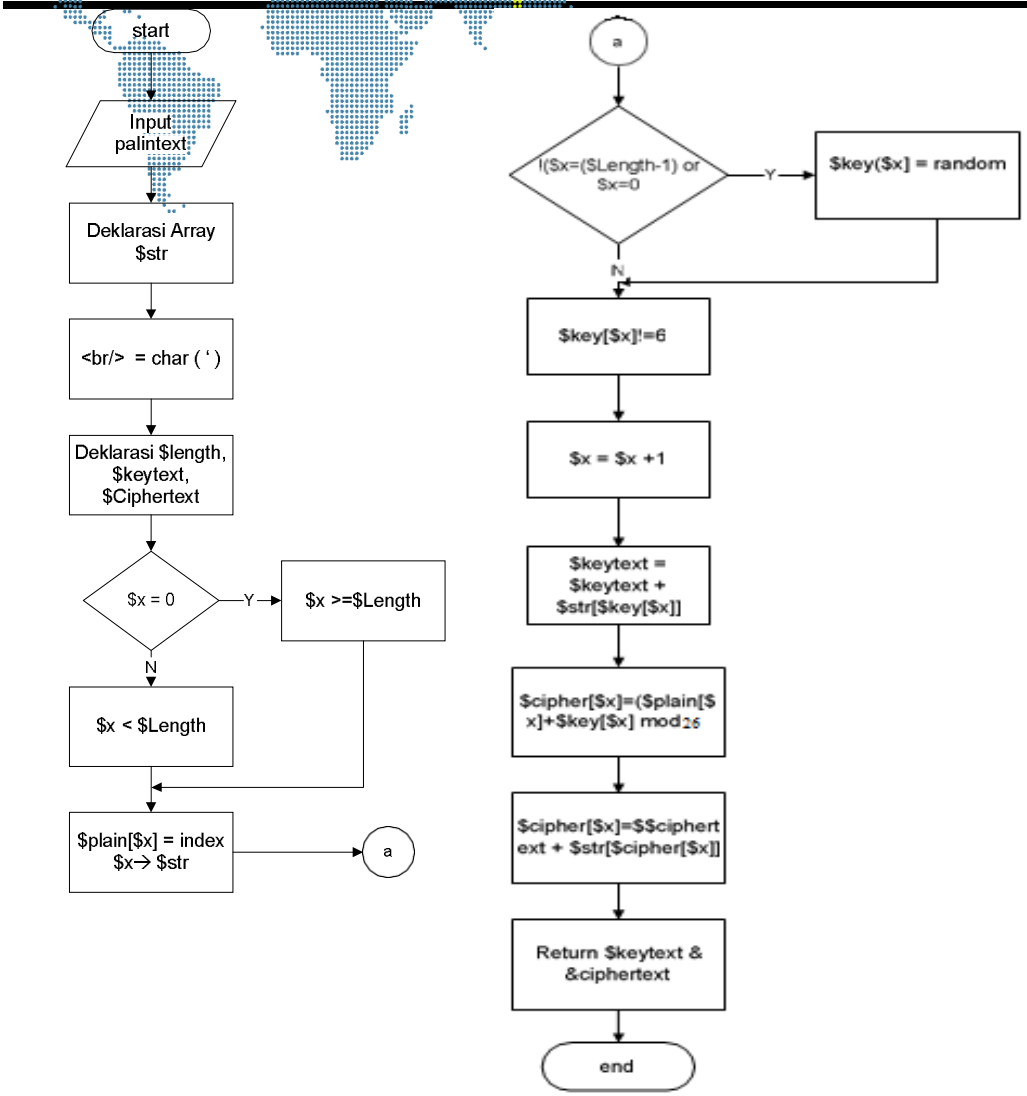
Langkah – langkah yang diperlukan untuk mencapai tujuan perancangan, yaitu :



Gambar 1. Bagan Alur Rancangan OTP

a) Melakukan perancangan aplikasi yang terdiri atas perancangan secara konseptual, perancangan aplikasi secara logis, dan perancangan secara fisik. Secara konseptual, akan ditentukan data/file yang dibuat pada *database* aplikasi.
    1) Membuat *Library* untuk proses Enkripsi *One Time Pad* dengan langkah-langkah sebagai berikut :
        1) Menerima data *plaintext* sebagai parameter dalam library
    2) Deklarasi *array $str* yang akan digunakan untuk menampung karakter – karakter yang diperbolehkan pada *plaintext* dan mengganti elemen html
 dengan karakter .
    3) Mendeklarasikan variabel *$length* (menampung data panjang *plaintext*), *$keytext* (menampung data kunci dan variabel), dan *$ciphertext* (menampung data *ciphertext* hasil enkripsi).
    4) Membuat perulangan sebanyak nilai dari variabel *$length*.
    5) Membuat kunci enkripsi. Kunci didapat dengan cara mengambil angka secara acak
    6) Membuat *ciphertext* dengan cara menjumlahkan indeks *plaintext* dengan kunci pada indeks yang sama lalu mod 26. Setelah *ciphertext* dan kunci didapatkan, program akan mengembalikan nilai berisi *ciphertext* hasil enkripsi dan kuncinya.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 588-597
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



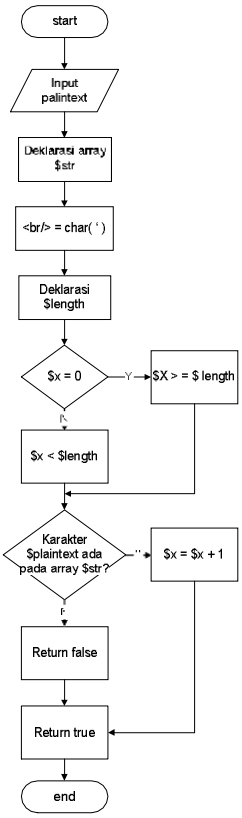
Gambar 2. *Flowchart* Enkripsi OTP

b) Membuat library untuk proses dekripsi pada ciphertext dengan langkah-langkah sebagai berikut :
   1) Menerima data ciphertext dan kunci sebagai parameter dalam library .
   2) Melakukan deklarasi $plaintext (menampung plaintext), $c_length (menampung data panjang ciphertext), dan $k_length (menampung data panjang kunci).
   3) Melakukan verifikasi kunci dengan membandingkan antara panjang kunci dengan panjang ciphertext. Pada kondisi panjang kunci dan panjang ciphertext tidak sama, maka kunci yang dimasukkan dinyatakan salah dan dalam hal ini library akan mengembalikan nilai false. Pada

kondisi panjang kunci sama dengan panjang ciphertext algoritma dilanjutkan dengan memberikan nilai ke variabel $key[$x] dengan indeks karakter key ke $x (variabel perulangan) pada array $str dan memberikan nilai ke variabel $cipher[$x] dengan indeks karakter ciphertext ke $x pada array $str.

4) Menghitung indeks plaintext dengan melakukan perhitungan $num = $cipher[$x] -$key[$x] dan jika $num lebih besar dari 0, indeks plaintext dapat diperoleh dengan $num mod 26. Pada kondisi $num bernilai negatif, nilai $num dijadikan positif dengan dikalikan dengan -1 lalu indeks plaintext dapat diperoleh dari hasil pengurangan 26 dikurangi $num.
5) Menambahkan karakter yang ada array $str ke variabel $plaintext sesuai dengan indeks plaintext hasil perhitungan.
6) Mengganti karakter ` dengan \r\n untuk mencetak spasi pada plaintext yang akan ditampilkan.

c) Mengembalikan data berupa plaintext hasil dekripsi.
d) Membuat *library* validasi *plaintext*, yang dapat dilihat pada diagram alir gambar 3.



Gambar 3. *Flowchart* Validasi Plaintext

Setelah dikonstruksi aplikasi akan diuji menggunakan dengan metode pengujian secara *Black Box Testing*. Metode ini menguji aplikasi terhadap berbagai masukan(*input*) yang terhadap fungsi-fungsi dari aplikasi untuk mengetahui apakah keluaran(*output*) proses seperti yang sudah direncanakan. Metode pengujian ini tidak memperhatikan struktur internal aplikasi. Pengujian akan menggunakan standar perangkat lunak yang telah disusun pada awal pembangunan sistem.

2.2. *File*

File atau berkas adalah sekumpulan berbagai informasi yang saling berhubungan dan tersimpan di dalam penyimpanan. Dan ada juga file yang bertipe program. Atau Definisi *file* adalah sekumpulan arsip ataupun data yang tersimpan di dalam komputer. *File* di komputer juga banayak tersimpan di dalam folder tertentu tergantung tempat penyimpan tersebut ingin dimana ia menyimpannya, setiap *file* juga memiliki ekstensi masing-masing tergantung jenis *file* itu sendiri. Ekstensi *file* adalah sebagai tanda yang membedakan jenis-jenis dari *file.*

Pada sistem operasi Unix dan Linux lainnya, segala sesuatu dalam sistem berbentuk *file*, termasuk direktori. Direktori (folder) menjadi suatu file khusus yang mengandung daftar dari nama-nama *file* beserta isi masing-masing. Direktori (folder) memiliki peran penting dalam sistem *file* pada sistem operasi komputer.

2.3. Algoritma *One Time Pad*

One-time pad (OTP) adalah suatu cipher aliran yang melakukan setiap enkripsi dan dekripsi satu karakter setiap kali. Algoritma ini ditemukan oleh Major Joseph Mauborgne pada tahun 1917 sebagai perbaikan dari algoritma Vernam cipher untuk menghasilkan keamanan yang lebih sempurna. Mauborgne mengusulkan penggunaan *one-time pad* (pad = kertas bloknot) yang berisi deretan karakter-karakter kunci yang dibuat secara acak. Satu pad hanya digunakan sekali (*one-time*) saja untuk menyandikan suatu pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain.

Penyandian(Enkripsi) dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci one-time pad:

$ci = (pi + ki) \bmod 26$ untuk alfabet 26-huruf (1)

Jika karakter yang digunakan adalah anggota himpunan 256 karakter (seperti karakter dengan pengkodean ASCII), maka persamaan enkripsinya menjadi:

$ci = (pi + ki) \bmod 256$ untuk alfabet 256-karakter (2)

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 588-597
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Penerima pesan menggunakan pad yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plainteks dengan persamaan:

pi = (ci – ki) mod 26 untuk alfabet 26-huruf, atau
pi = (ci – ki) mod 256 untuk alfabet 256-karakter. (3)

3. HASIL DAN PEMBAHASAN

3.1. Analisis & Hasil Uji Coba

Data yang digunakan dalam penelitian berupa file-file data yang berjenis pengolah kata (*doc*),(*docx*) dan teks (*txt*). File-file ini digunakan untuk menguji aplikasi. Keseluruhan jumlah file yang digunakan adalah 3 buah file dengan rincian sebagai berikut: Tabel 1.

Tabel 1. File Data Untuk Pengujian

No	Nama File	Jenis	Ukuran (KB)
1	Data.txt	txt	1
2	Abstrak.doc	doc	24
3	Memo.docx	docx	82

Seperti rancangan yang telah dibuat, file-file *doc, pdf,* dan *txt* dengan ukuran 100 KB kebawah telah berhasil dienkripsi maupun didekripsi dengan kecepatan dibawah 1 detik. 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 berubah sebagai berikut:

Tabel 2. Hasil Uji Menunjukkan Ukuran File Uji Tidak Berubah

No	File Uji	Ukuran File Sebelum Enkripsi	Ukuran File Setelah Enkripsi	Kesimpulan
1	Data.txt	1 KB	1 KB	Valid
2	Abstrak.doc	24 KB	1 KB	Valid
3	Memo.docx	82 KB	1 KB	Valid

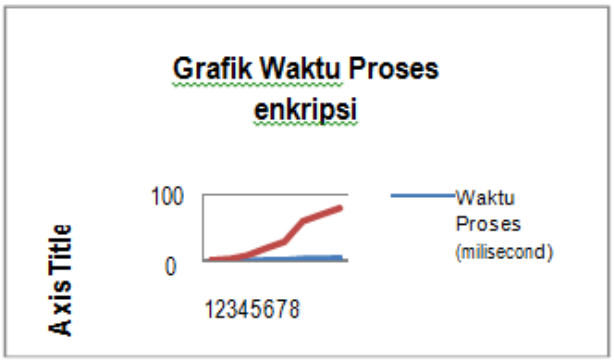
Tabel 5 menunjukkan hasil uji coba implementasi algoritma OTP dengan ukuran *file* sebelum proses enkripsi dengan ukuran *file* setelah proses enkripsi, dimana mengalami perubahan. File ujicoba berformat .txt.

Tabel 3. Waktu Pengujian *file* setelah enkripsi

Waktu Proses (Milisecond)	15	20	55

Ukuran File (byte)	1	1	1

Kecepatan proses enkripsi dan dekripsi dipengaruhi dari kapasitas file dimana grafik hasil ujicoba dapat dilihat pada gambar 4.



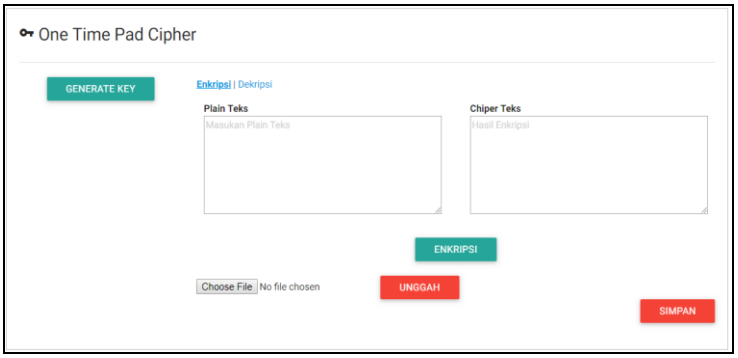
Gambar 4. Grafik waktu proses enkripsi

3.2. Hasil

Berikut ini dijelaskan tentang tampilan hasil dari Aplikasi Keamanan *File Teks* Menggunakan Kriptografi Dengan Algoritma *One Time Pad* (OTP). dapat dilihat sebagai berikut :

a) Tampilan *Menu Utama*

Fungsi dari tampilan adalah untuk menampilkan halaman awal dari aplikasi yang telah dibangun. Tampilan pada *Menu utama* dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar 5 berikut:

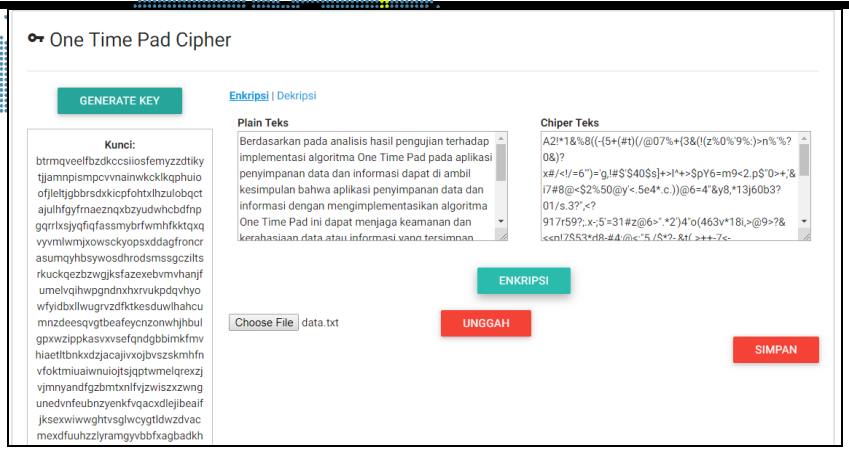


Gambar 5. Tampilan *Menu utama*

b) Tampilan *Enkripsi*

Fungsi dari tampilan *Enkripsi* adalah memilih data audio yang akan dilakukan enkripsi data. Tampilan pada *form Enkripsi* dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar 6 berikut :

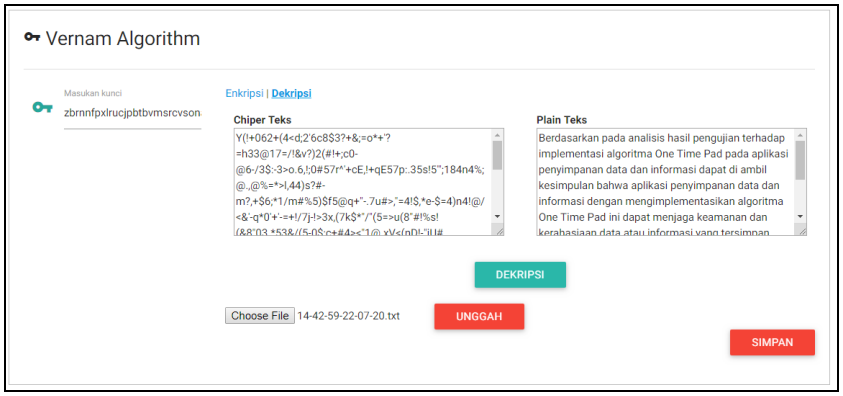
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 588-597
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 6. Tampilan *Enkripsi*

c) Tampilan *Dekripsi*

Fungsi dari tampilan *Dekripsi* adalah melakukan dekripsi data terhadap data audio yang telah di enkripsikan terlebih dahulu. Tampilan pada *form Dekripsi* dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar 7 berikut:



Gambar 7. Tampilan *Deskripsi*

4. SIMPULAN

Aplikasi pengaman file teks berbasis web ini menggunakan chiper yang terbukti sulit untuk di pecahkan (*unbreakable)* dengan panjangnya kunci dan password sekali pakai. Dari teknik enkripsi yang digunakan, ketahanan dan keamanan proteksi terhadap data pribadi sudah 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. Pengujian dengan metode blackbox memastikan aplikasi

telah berjalan sesuai spesifikasinya. Agar keamanan data pribadi terutama file teks lebih terjamin lagi.

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 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] Muhammad Reza Fahlevi (2017), Aplikasi Keamanan Folder Menggunakan Kriptografi Dengan Algoritma One Time Pad (Otp), DSpace JSPUI.

[2] De Rosal Ign ,et al (2017*),* Implementasi One Time Pad Kriptografi Pada Gambar Grayscale Dan Gambar Berwarna, Prosiding Seminar Multi Disiplin, ISBN : 9-789-7936-499-93.

[3] Heri Santoso, Mhd. Zulfansyuri Siambaton (2020), Aplikasi Pengamanan Ekstensi File Menggunakan Kriptografi One Time Pad (Otp) Dan Elliptic Curve Cryptography (Ecc)" *JISTech (Journal of Islamic Science and Technology*. ISSN: 2528-5718.

[4] Lalang Erawan, Suharnawi (2018), Implementasi Algoritma One Time Pad Untuk Proteksi File Data Pribadi Pada Aplikasi Berbasis Web , *Journal of Information System, Vol 03. No.02 Nopember 2018.*

[5] Hernalom, Belathika Gornea (2016), Teknik Keamanan File Menggunakan Kriptografi Dengan Algoritma Vernam Cipher*, Jurnal Satya Informatika, Vol. 1 No. 2, September 2016 Halaman 1-13*

[6] Munir, Rinaldi (2011), Algoritma Enkripsi Citra Dengan Pseudo One Time Pad Yang Menggunkan Sistem Chaos, *Konferensi Nasional Informatika.* ISSN : 2087-3328 : 12-16

[7] M.Sholeh, et all (2011), Aplikasi Kriptografi Dengan MetodeVernam Chiper Dan Metode Permutasi Biner, *Institut Sains & Teknologi AKPRIND Yogyakarta.* Momentum, Vol.7 No.2, Oktoer 2011 : 8- 13