Pengamanan Data Teks Dengan Menggunakan Algoritma Zero-Knowledge Proof

Rozali Toyib[1], Yulia Darnita[2]

Dosen Tetap Program Studi Teknik Informatika Fakultas Ilmu Teknik Universitas Muhammadiyah Bengkulu
Alamat (Telp. (0736) 22765, Fax. (0736) 26161; e-mail:rozalitoyib@umb.ac.id)

[1,2,] Dosen Tetap Program Studi Teknik Informatika Fakultas Ilmu Teknik Universitas Muhammadiyah Bengkulu
Jl. Bali Po.Box, 118 Kota Bengkulu 38119 Telp. (0736) 22765, Fax. (0736) 26161; e-mail:yuliadarnita@umb.ac.id)

Abstract - Data security is very important in maintaining the confidentiality of the information itself, especially if the information is only known by certain parties. Sending data or information without security will be at risk of being tapped. So that the information contained in it can be easily known by unauthorized parties, and things like that are very detrimental. Until now, cryptography is one of the solutions to ensure the security of information. Zero Knowledge Proof (ZKP) is a cryptographic protocol that can be used by someone to prove someone's ownership (prover) of confidential information to others (verifier), without the need to disclose the information or provide a way for other people to find out the secret. The test result is Zero Knowledge Proof divides one data stream into small blocks. Each of these blocks is encrypted separately. In an implementation without proof of knowledge, the key to encrypt will only be with the user, and by that, he will be able to encrypt and decrypt the information. Zero knowledge proof algorithm is a unique method by which the user can prove to other users that he knows additional information.
Keywords: Security, data, wiretapping, Zero-Knowledge proof

Intisari - Keamanan data sangat penting dilakukan dalam menjaga kerahasiaan informasi itu sendiri, terutama bila informasi tersebut hanya boleh diketahui pihak yang tertentu saja. Pengiriman data atau informasi tanpa dilakukan pengamanan akan beresiko terhadap penyadapan. Sehingga informasi yang ada di dalamnya dapat mudah diketahui oleh pihak-pihak yang tidak berhak, dan hal seperti itu sangat merugikan.Hingga saat ini, kriptografi merupakan salah satu solusi untuk menjamin keamanan dari suatu informasi. Zero Knowledge Proof (ZKP) merupakan protokol kriptografi yang dapat digunakan seseorang untuk membuktikan kepemilikan seseorang (prover) akan suatu informasi rahasia kepada orang lain (verifier), tanpa perlu mengungkapkan informasi tersebut atau memberikan cara bagi orang lain untuk mengetahui rahasia tersebut. Hasil pengujian adalah Zero Knowledge Proof membagi satu aliran data menjadi blok-blok kecil Masing-masing blok ini dienkripsi secara terpisah. Dalam implementasi tanpa bukti pengetahuan, kunci untuk mengenkripsi hanya akan berada pada pengguna, dan dengan itu, ia akan dapat mengenkripsi dan mendekripsi informas, Algoritma zero knowledge proof adalah metode yang unik dimana pengguna dapat membuktikan kepada pengguna lain bahwa dia tahu informasi tambahan.
Kata Kunci: Keamanan ,data,penyadapan ,Zero-Knowledge proof

I. PENDAHULUAN

Keamanan data sangat penting dilakukan dalam menjaga kerahasiaan informasi itu sendiri, terutama bila informasi tersebut hanya boleh diketahui pihak yang tertentu saja. Pengiriman data atau informasi tanpa dilakukan pengamanan akan beresiko terhadap penyadapan. Sehingga informasi yang ada di dalamnya dapat mudah diketahui oleh pihak-pihak yang tidak berhak, dan hal seperti itu sangat merugikan.Hingga saat ini, kriptografi merupakan salah satu solusi untuk menjamin keamanan dari suatu informasi.

Kriptografi merupakan salah satu metode yang dapat digunakan dalam menyelesaikan masalah keamanan data dengan menyandikan isi informasi (plaintext) menjadi isi yang sulit atau bahkan tidak dipahami melalui proses enkripsi. Untuk memperoleh kembali informasi yang asli dapat dilakukan dengan proses dekripsi, yang tentunya dengan menggunakan kunci yang benar.

Hasil yang didapat dari sistem kriptografi bisa melindungi akses datadari pihak-pihak yang tidak berkepentingan maka sangat diperlukan enkripsi dan dekripsi dalam pengamanan data. Agar dapat dilakukan dengan baik, dibutuhkan suatu algoritma untuk enkripsi dan dekripsi.Algoritma yang digunakan disini adalah Algoritma zero-knowledge.

Kriptografi (Cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia.Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan.Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data [1].

Zero Knowledge Proof (ZKP) merupakan protokol kriptografi yang dapat digunakan seseorang untuk membuktikan kepemilikan seseorang (prover) akan suatu informasi rahasia kepada orang lain (verifier), tanpa perlu mengungkapkan informasi tersebut atau memberikan cara bagi orang lain untuk mengetahui rahasia tersebut [2].

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya [3].

II. TINJAUAN PUSTAKA

A. Kriptografi

Pengertian Kriptografi dalam kamus bahasa Inggris Oxford adalah sebagai berikut : " Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan mengguanakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini [4].Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan [5].

B. Algoritma Zero-Knowledge

Zero Knowledge Proof atau ZKP adalah metode interaktif yang digunakan untuk melakukan autentifikasi dari dokumen pihak lain tanpa memperlihatkan realita lainnya [6].Protokol Zero Knowledge Proof merupakan salah satu protokol dalam Kriptografi yang memiliki tingkat keamanan yang cukup baik, karena menerapkan konsep "Truly Zero Knowledge Proof" yaitu tidak membocorkan informasi apapun. Protokol ini digunakan pada Algoritma Feige Fiat Shamir, Guillou Quisquater dan Schnorr, ketiganya merupakan Algoritma Kriptografi dengan menggunakan kunci privat dan kunci publik. Pada kunci Publik, ketiga Algoritma ini menggunakan pembangkit bilangan prima acak pada nilai p dan q untuk mendapatkan kunci publik.Untuk memastikan bilangan yang dipilih merupakan bilang prima, maka digunakan metode Rabin Miller untuk melakukan pengetesan [7].

C. Keamanan Data

Keamanan data adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi[8].

Keamanan data dapat dibedakan menjadi dua kategori, yaitu keamanan fisik dan keamanan sistem. Keamanan fisik merupakan bentuk keamanan berupa fisik dari server, terminal/client router sampai dengan cabling. Sedangkan keamanan sistem adalah keamanan pada sistem pengoperasiannya atau lebih khususnya pada lingkup perangkat lunak, misalnya dengan penggunaan kriptografi dan steganografi [9]

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi.Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi.Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting [10]. Salah Satu hal terpenting dalam komunikasi menggunakan computer dan jaringan computer adalah untuk menjamin keamanan pesan, data ataupun informasi dalam proses pengiriman dan penyimpanan data [11].

Data bisa juga didefinisikan sekumpulan informasi atau nilai yang diperoleh dari pengamatan (observasi) suatu obyek , data dapat berupa angka dan dapat pula merupakan lambang atau sifat [12]

Data Integrity, adalah memastikan bahwa informasi dan program yang diubah hanya dengan cara tertentu dan berwenang. System Integrity, adalah memastikan bahwa sistem melakukan fungsi yang ditujukan secara tak terhalang, bebas dari manipulasi yang tidak sah disengaja atau tidak di sengaja dari sistem.Availability yaitu meyakinkan bahwa sistem bekerja segera dan layanan tidak di tolak untuk pengguna yang berwenang [13].

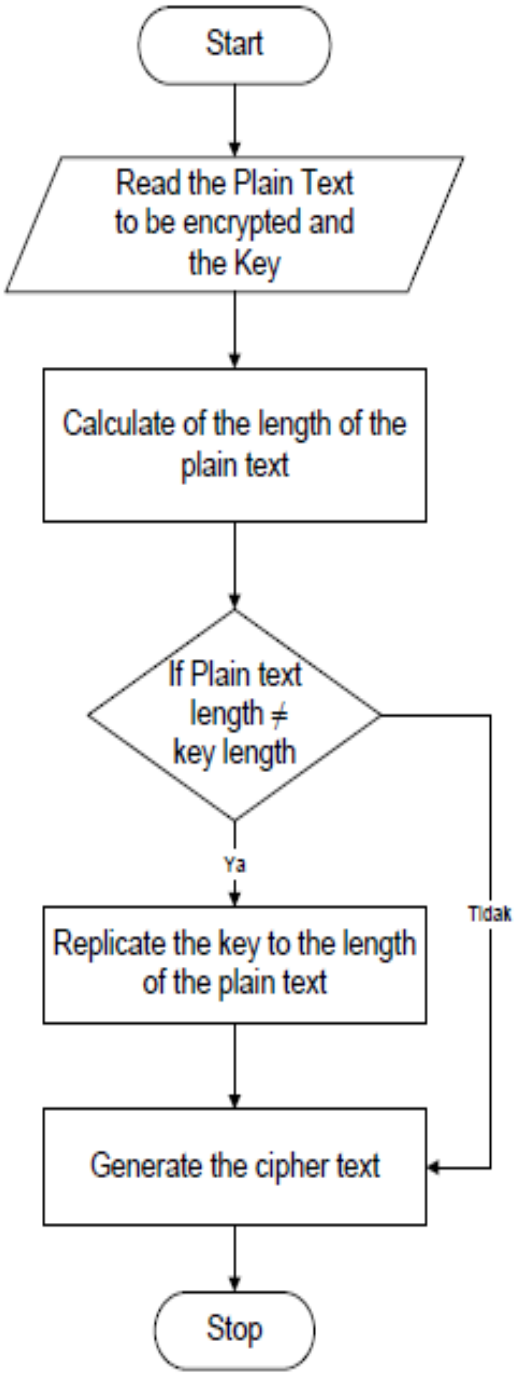
III. METODO PENELITIAN

A. Metode Pengembangan Sistem

Pengembangan sistem didefinisikan sebagai aktivitas untuk untuk menyelesaikan persoalan (problem) organisasi atau memanfaatkan kesempatan organisasi atau memanfaatkan kesempatan (opportunities) yang timbul. Model Air Terjun (waterfall):

1. Rekayasa perangkat lunak (*system enginerring*), melakukan pengumpulan data dan penetapan kebutuhan semua elemen system
2. *Requirements analysis*, melakukan analisis terhadap permasalahan yang dihadapi dan menetapkan kebutuhan perangkat lunak, fungsi performsi dan interfacing
3. design, menetapkan domain informasi untuk perangkat lunak,fungi dan interfacing
4. Coding (imolementasi), pengkodean yang mengimplementasikan hasil desain ke dalam kode atau bahasa yang dimengerti oleh mesin komputer dengan menggunakan bahasa pemprograman tertentu.
5. Testing (pengujian), kegiatan untuk melakukan pengetesan program yang sudah dibuat apakah udah benar atau belum di uji dengan cara manual.jika testing sudah benar maka program boleh digunakan
6. Maintenance (perawatan) , menangani perangkat lunak yang sudah selesai supaya dapat berjalan lancar dan terhindar dari gangguan-gangguan yang dapat menyebabkan kerusakan

B. Flowchart



Gambar 1. Flowchart Algoritma zero-knowledge

C. Analisis Protokol Zero Knowledge Proof

Dalam pengamanan data mmenggunakan Algoritma *zero-knowledge* data yg digunakan berupa text dengan panjang 80 karakter. Metode yg digunakan Polygram iyalah sistem asimetris (tidak simetris) menggunakan beberapa key untuk pengenkripsian yaitu

public key untuk enkripsi data dan private key untuk dekripsi data. Public key disebarkan ke seluruh dunia sementara private key tetap disimpan. Siapapun yang memiliki public key tersebut dapat mengenkripsi informasi yang hanya dapat dibaca oleh seseorang yang memiliki private key walaupun anda belum pernah mengenal bahkan tidak tahu sama sekali siapa yang memiliki public key tersebut.“

Read the Plain Text to be encrypted and the Key
Calculate of the length of the plain text
If Plain text length ≠ key length
If Right
Than Replicate the key to the length of the plain text
AndGenerate the cipher text
If false
Than Generate the cipher text
End

Ada tiga bentuk tahapan yang digunakan dalam pembuktian interaktif dengan menggunakan metode ZKP yaitu:

1. Witness yaitu prover/signer memilih suatu bilangan random dan mengirimkannya ke verifier yang dapat membuktikan bahwa prover mengetahui informasi rahasia.Bilangan tersebut mendefinisikan suatu pertanyaan yang harus dijawab oleh prover/signer.
2. Challenge yaitu verifier memilih pertanyaan acak dan mengirimkannya ke prover/signer.
3. Response yaitu prover menjawab pertanyaan verifier dengan menggunakan informasi rahasia yang dimilikinya.

Tahapan ini akan dilakukan terus menerus dalam beberapa kali perulangan, tujuannya yaitu untuk mengurangi kemungkinan prover benar hanya karena menebak jawaban yang kebetulan benar. Dalam suatu sistem otentikasi berbasis ZKP, terdapat persyaratan sebagai berikut :

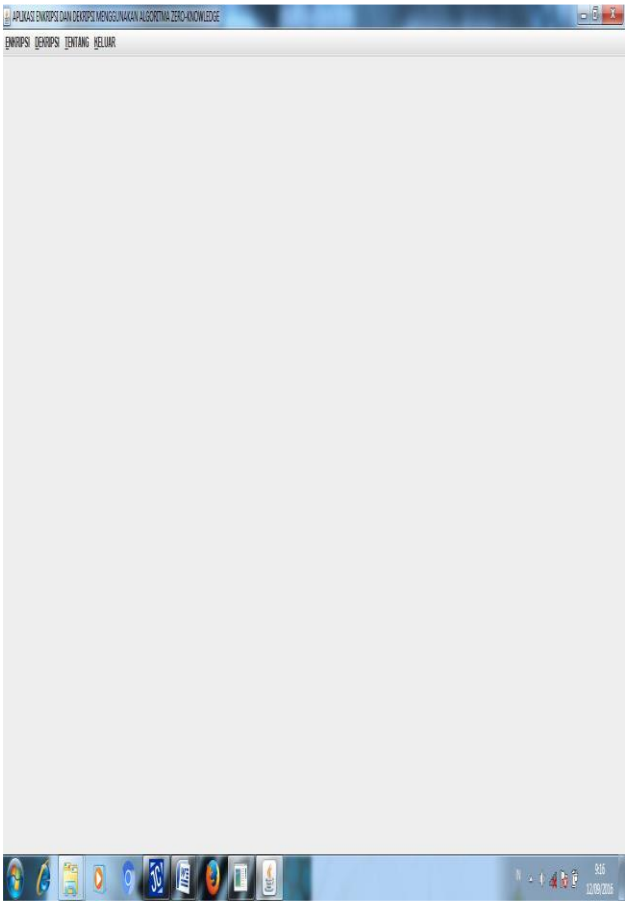
1. Completeness, jika pernyataannya benar, maka prover/signer yang asli dapat membuktikan bahwa pernyataannya benar kepada verifier setiap waktu.
2. Soundness, jika pernyataannya salah, maka tidak mungkin untuk memalsukan hasil kepada verifier bahwa pernyataannya benar.
3. Zero-Knowledge yaitu apabila pernyataannya betul, pihak Verifier tak mengetahui apapun kecuali pernyataannya benar. Informasi rahasia dibalik pernyataan tidak akan diungkapkan.

IV. HASIL DN PEMBAHASAAN

A. Hasil

a. Menu Utama

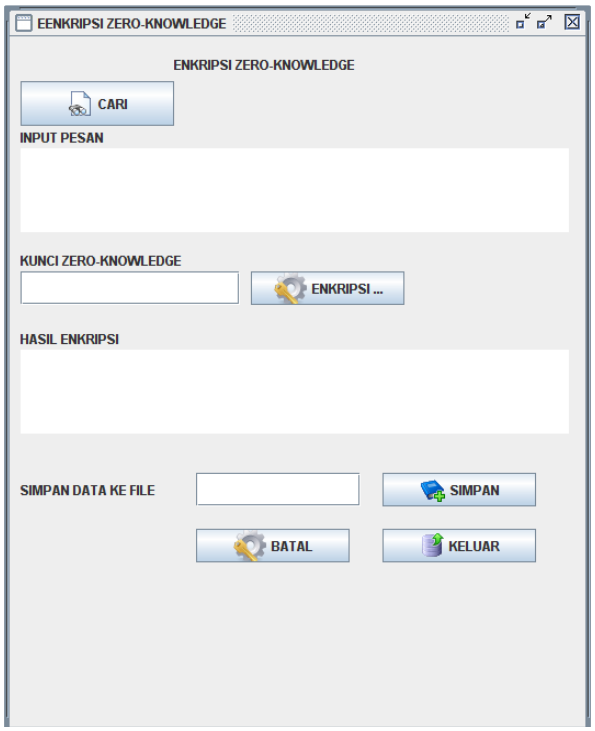
Tampilan Menu utama ini terdiri atas menu enkripsi dan menu dekripsi, menu enkripsi untuk merubah plainteks menjadi chiperteks sedangkan menu enkripsi untuk mengembalikan pesan chiperteks menjadi pesan plainteks kembali.Menu tentang pada aplikasi ini merupakan info kegunaan dari aplikasi itu sendiri dan menu keluar yang digunakan untuk mengakhiri kegiatan pada aplikasi ini.



Gambar 2. Tampilan Menu Utama

b. Menu Enkripsi

Menu enkripsi berisi form yang digunakan untuk mengubah pesan dari plainteks menjadi pesan chiperteks, dengan memasukan pesan yang ingin di ubah kemudian memasukan kunci pesan dan kmudian melakukan proses enkripsi pesan plainteks yang di masukan sebelumya berubah menjasi bahasa sandi atau chiperteks.

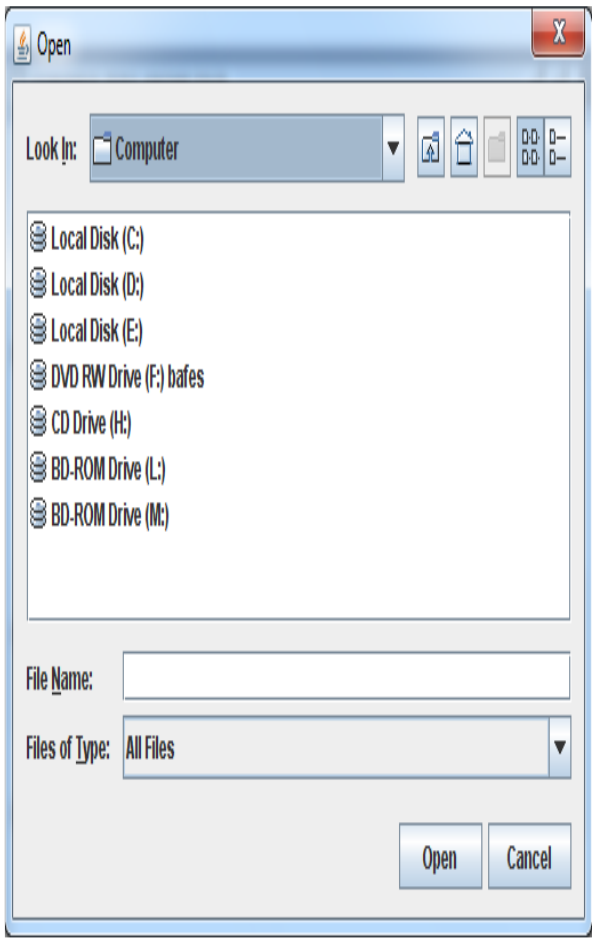


Gambar 3. Menu Proses Enkripsi Pada Algoritma *Zero-knowledge.*

Pada menu ini terdapat 5 (lima) buah tombol yang memiliki fungsi masing- masing yaitu:

1. Tombol Cari

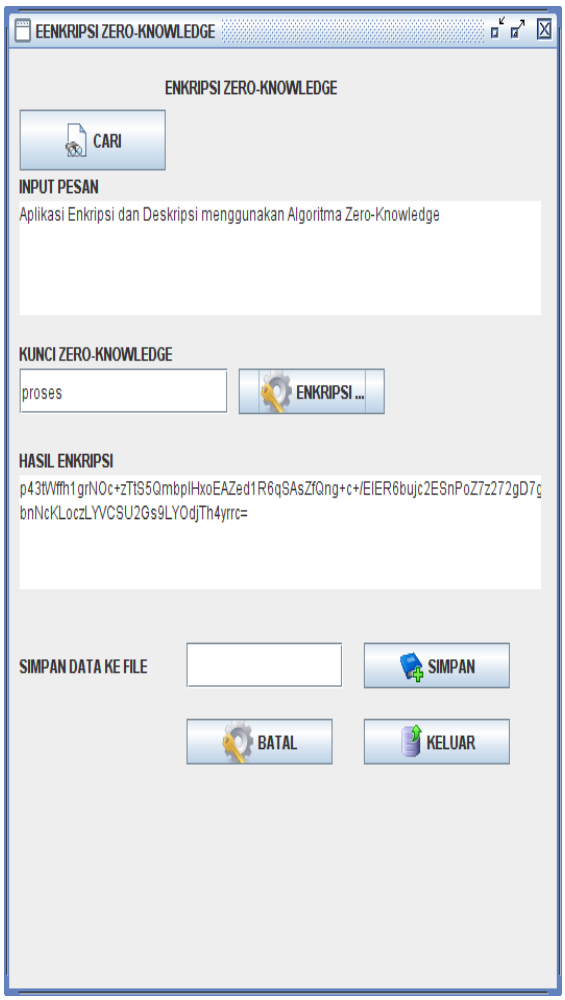
   Tombol cari digunakan untuk mencari file yang ingin di enkripsikan, file yang bisa di masukan keladam proses enkripsi adalah format data *txt.



Gambar 4.Proses pencarian pesan yang ingin di enkripsi

2. Tombol Proses

   Tombol proses digunakan untuk menjalankan proses enkripsi pada aplikasi kriptografi algoritma *zero-knowledge* setelah memasukan pesan plaintext pada textfile dan memasukan kunci pada textfile kunci yang akan di proses menjadi chipertext yang akan di tunjukan pada textfile hasil enkripsi adapun proses-porsesnya seperi berikut.



Gambar 5. Hasil Enkripsi Algoritma *Zero-knowledge*

Pada gambar 5 menunjukan hasil dari proses enkripsi algoritma *zero-knowledge*.

3. Tombol Simpan

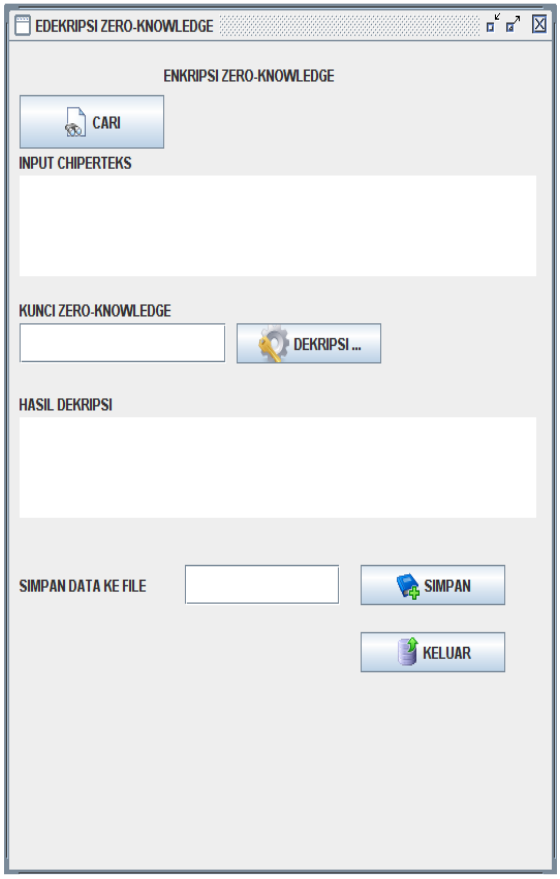
   Pada tombol simpan merupakan tombol untuk menyimpan hasil enkripsi yang telah menjadi chipertext dengan memberikan judul file pada textfile simpan data maka data secara langsung akan tersimpan pada localdics D:/.

4. Tombol Keluar

   Tombol keluar merupakan tombol untuk proses keluar dari halaman

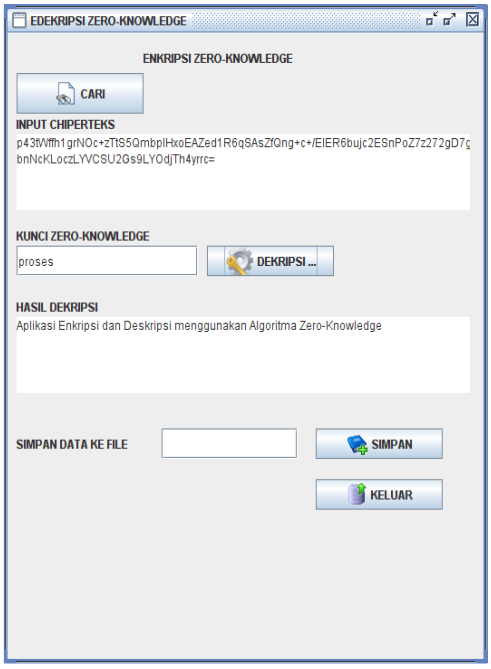
c. Menu Dekripsi

Menu ini berisi halaman yang digunakan untuk dekripsi pesan dan decoding, pesan rahasia yang akan merubah pesan chipertext menjadi pesan plaintext kembali.



Gambar 6. Halaman Dekripsi

Dengan membuka file yang di simpan pada localdics D:/ dan memasukan file kedalam textfile chipertext dan memasukan kunci pesan lalu 38 melanjutkan proses dari dekripsi. Berikut ini adalah hasil dari Dekripsi pesan dan Dekoding.



Gambar 7. Proses dekripsi

B. Pembahasaan

a. Black Box

Pengujian black-box berfokus pada pengujian persyaratan fungsional perangkat lunak, untuk mendapatkan serangkaian kondisi input yang sesuai dengan persyaratan fungsional suatu program. Pengujian black-box ini dilakukan pada program utama yaitu pada menu enkripsi dan encoding dengan menu dekripsi.

Tabel 4.1 Pengujian Sistem enkripsi dan dekripsi

Input/Event	Output	Hasil
Tombol cari	Pencarian datang yang ingin di enkripsi atau di dekripsi	Sesuai
tombol proses	Enkripsi dekripsi pesan rahasia dari pesan pada algoritma *zero-knowledge*.	Sesuai
tombol simpan	penyimpanan pesan yang sudah di enkripsi ataupun dekripsi kedalam bentuk .txt*	Sesuai
tombo lkeluar	Untuk keluar dari proses enkripsi data dalam aplikasi kriptografi menggunakan algoritma *zero-knowledge*	Sesuai

b. Manual Sistem

$K = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix}$

$P = \begin{Bmatrix} 16 \\ 1 \end{Bmatrix} \begin{Bmatrix} 19 \\ 19 \end{Bmatrix} \begin{Bmatrix} 23 \\ 15 \end{Bmatrix} \begin{Bmatrix} 18 \\ 14 \end{Bmatrix} \begin{Bmatrix} 18 \\ 1 \end{Bmatrix} \begin{Bmatrix} 19 \\ 9 \end{Bmatrix}$

$e = K.P\ Mod\ 26$

$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (16 \quad 1) mod\ 26$

$= (16.1 + 1.19\ 16.12 + 1.9)$ mod 26

$= (35\ \ 201) mod\ 26$

$= (35\ mod\ 26\ 201\ mod\ 26)$

$= (9\ 19) = I\ S$

$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (19 \quad 19) mod\ 26$

$= (19.1 + 19.19\ 16.12 + 19.9)$ mod 26

$= (380\ 399)$

$= (380\ mod\ 26\ 399\ mod\ 26)$

$= (16\ 9) = P\ I$

$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (23 \quad 15) mod\ 26$

$= (23.1 + 15.19\ 23.12 + 15.9)$ mod 26

$= (380\ 411)\ mod\ 26$

$= (22\ 21) = V\ U$

$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (18 \quad 4) mod\ 26$

$= (94\ 252)$mod 26

$= (94\ mod\ 26\ 252\ mod\ 26)$

$= (16\ 18) = P\ R$

$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (18 \quad 1) mod\ 26$

$= (18.1 + 1.19\ 18.12 + 9.1)$ mod 26

$= (194\ mod\ 26\ 309\ mod\ 26)$

$= (8\ 23) = H\ W$

Hasil enkripsi secara menyeluruh dari teks yang disebut dengan *plantext* "PASSWORD RASI" dan *key* K yang digunakan "ASLI" menghasilkan proses enkripsi dengan teks atau yang disebut *chipertext* "ISPIVUPRKQHW setelah mendapatkan enkripsi maka hasil di ubah ke bahasa mesin n8HL532SljyXhf+PL0/mDg== ".

V. KESIMPULAN

1. Algoritma zero knowledge proof adalah metode yang unik dimana pengguna dapat membuktikan kepada pengguna lain bahwa dia tahu informasi tambahan.
2. Seseorang dapat membuktikan bahwa diatahu nilai z ke orang lain tanpa memberi informasi selain fakta bahwa dia tahu nilaiznya.
3. Zero Knowledge Proof membagi satu aliran data menjadi blok-blok kecilMasing-masing blok ini dienkripsi secara terpisah. Dalam implementasi tanpa bukti pengetahuan, kunci untuk mengenkripsi hanya akan berada pada pengguna, dan dengan itu, ia akan dapat mengenkripsi dan mendekripsi informas

DAFTAR PUSTAKA

[1] Amin, M. M. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Pseudocode*, *3*(2), 129-136.

[2] Raharjo, W. S., & Sutanti, D. (2015).Implementasi Zero Knowledge Proof Menggunakan Protokol Feige Fiat Shamir Untuk Verifikasi Tiket

Rahasia. *Ultimatics: Jurnal Teknik Informatika*, *7*(2), 91-97.

[3] Permana, A. A., & Nurnaningsih, D. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). *JURNAL TEKNIK INFORMATIKA*, *11*(2), 177-186.

[4] Zelvina, A., Effendi, S., & Arisandi, D. (2012). Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa. *Dunia Teknologi Informasi-Jurnal Online*, *1*(1).

[5] Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20-31.

[6] Putro, H. P. Percobaan Pemanfaatan Graf pada Protokol Kriptografi. *Program Studi Teknik Informatika STEI ITB, Bandung*, *40135*.

[7] Panjaitan, C. (2019). Analisis Pola Identifikasi Zero Knowledge Proof dengan Algoritma Feige Fiat Shamir, Guillou Quisquater dan Schnorr pada Sistem Keamanan Informasi.

[8] Kurniawan, Agus. 2008. *Konsep dan Implementasi Pengamanan Data Dengan* .NET. Jakarta: PC Media

[9] Kurniawan, Yusuf. 2009. *Kriptografi Keamanan Internet dan jaringan Telekomunikasi.*Bandung: Penerbit Informatika.

[10] Rahardjo, B. (2005). Keamanan sistem informasi berbasis internet. *Jakarta: PT INDOCISC.*.

[11] Haji, W. H., & Mulyono, S. (2012). Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data. *Jurnal Fakultas Hukum UII*.

[12] Rusmana, A. (2014). Analisis Sistem Informasi.

[13] Yuliansyah, H. (2014). Perancangan replikasi basis data mysql dengan mekanisme pengamanan menggunakan ssl encryption. *Jurnal Teknik Informatika*.(2002)