Jurnal Cyber Tech
Vol.1. No.2, Mei 2018, pp. x~x
P-ISSN:1978-6603
E-ISSN:2615-3475

Aplikasi Kriptografi Keamanan Dokumen Dinas Perhubungan Provinsi Sumatera Utara Dengan Algoritma AES *(Advanced Encryption Standard)* Berbasis *Web*

Vicky Ulfa Romyata Sembiring (First Author)*, Badrul Anwar,S.E,S.Kom.,M.Kom., Ismawardi Santoso,S.Kom.,M.Kom.****
* Program Studi Mahasiswa, STMIK Triguna Dharma
** Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info
Article history:
Received Jun 12th, 201x
Revised Aug 20th, 201x
Accepted Jan 21th, 201x

Keyword:
Dinas Perhubungan
Aplikasi Kriptografi
Kriptografi
Advance Encryption Standard
File Dokumen

ABSTRACT
Dinas Perhubungan Provinsi Sumatera Utara adalah suatu instansi pemerintah yang mempunyai tugas serta ada beberapa urusan rumah tangga pemerintah daerah dan pembantuan di bidang perhubungan, khususnya di Sub Bagian Umum. Dalam hal ini permasalahan yang terjadi pada dinas perhubungan provinsi sumatera utara mempunyai isi data *file* dokumen yang sangat penting yaitu perihal mengenai informasi surat keputusan dalam proses pemindahan jabatan lama dan penugasan jabatan baru pada pegawai dinas perhubungan provinsi sumatera utara dalam bentuk *format* docx. Pegawai dapat melakukan kecurangan mengubah isi data dan melihat serta memodifikasi isi data *file* dokumen tersebut. Maka terjadinya kesalahan pemahaman informasi dalam proses pemberian pelaksanaan pemindahan jabatan lama dan penugasan jabatan baru pada pegawai dinas perhubungan provinsi sumatera utara. Dalam hal ini supaya bisa mencegah dan menangani tidak terjadinya permasalahan tersebut, maka perlu dibangun sebuah sistem aplikasi keamanan data yang mampu mengamankan isi *file* dokumen dengan menggunakan teknik yaitu kriptografi. Algoritma kriptografi yang digunakan yaitu algoritma *Advanced Encryption Standard*. Hasil pengujian menunjukkan bahwa sistem aplikasi keamanan dokumen dinas perhubungan provinsi sumatera utara dapat menjamin isi data *file* dokumen informasi perihal mengenai pemindahan jabatan lama dan penugasan jabatan baru pegawai bersifat rahasia dalam bentuk *chipertext* dan tersimpan di *database* dari pihak pegawai yang tidak berwenang.

Corresponding Author:*First Author
Nama : Vicky Ulfa Romyata Sembiring
Program Studi Sistem Informasi
STMIK Triguna Dharma
Email: vickyromyata@gmail.com

1. PENDAHULUAN

Dinas Perhubungan Provinsi Sumatera Utara adalah suatu instansi pemerintah yang mempunyai tugas serta ada beberapa urusan rumah tangga pemerintah daerah dan pembantuan di bidang perhubungan, khususnya di Sub Bagian Umum sudah menerapkan teknologi komputer dalam proses pengelolaan data dokumen seperti urusan surat-menyurat, administrasi kepegawaian dan inventarisasi barang-barang. Seluruh data-data tersebut dalam bentuk *format* .docx, .pptx .xlsx, serta berupa gambar .png, dan .jpeg.

Dalam hal ini permasalahan yang terjadi pada dinas perhubungan provinsi sumatera utara mempunyai isi data *file* dokumen yang sangat penting yaitu perihal mengenai informasi surat keputusan dalam proses pemindahan jabatan lama dan penugasan jabatan baru pada pegawai dinas perhubungan provinsi sumatera utara dalam bentuk *format* docx. Pegawai dapat melakukan kecurangan mengubah isi data dan melihat serta

memodifikasi isi data *file* dokumen tersebut. Maka terjadinya kesalahan pemahaman informasi dalam proses pemberian pelaksanaan pemindahan jabatan lama dan penugasan jabatan baru pada pegawai dinas perhubungan provinsi sumatera utara.

Untuk mencegah serta menangani tidak terjadinya perihal permasalahan tersebut, maka perlu dibangun sebuah sistem aplikasi keamanan data yang mampu mengamankan isi data *file* dokumen dengan menggunakan teknik yaitu kriptografi. Menurut Arief, M., dkk (2015:46) Kriptografi mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Algoritma kriptografi merupakan langkah-Iangkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut.

Banyak algoritma yang bisa digunakan pada kriptografi, salah satunya adalah AES *(Advanced Encryption Standard)*. Dalam ilmu kriptografi algoritma *AES (Advanced Encryption Standard)* ini merupakan kunci simetris yang cukup kuat dalam keamanannya dan pengkodeannya sangat sukar untuk dipecahkan. Salah satu cara yang digunakan untuk menjamin keamanan isi data informasi perihal mengenai pemindahan jabatan lama dan penugasan jabatan baru pada pegawai yaitu enkripsi dan dekripsi *file* dokumen dilakukan pada saat proses penyimpanan di dalam *database* serta supaya menghasilkan isi data yang bersifat rahasia dalam bentuk *chipertext*.

2. METODE PENELITIAN

2.1 *Advance Encryption Standard (AES)*

Pada tahun 1997 kontes pemilihan suatu standar algoritma kriptografi baru pengganti DES dimulai dan diikuti oleh 21 peserta dari seluruh dunia.Setelah melewati tahap seleksi yang ketat, pada tahun 1999 hanya tinggal 5 calon yaitu algoritma *Serpent* (Ross Anderson-*University of* Cambridge, Eli Biham-*Technion,* Lars Knudsen-*University of* California San Diego), *MARS* (IBM Amerika), *Twofish* (Bruce Schneier, John Kelsey, dan Niels Ferguson-*Counterpane Internet Security Inc, Doug Whiting-Hi/fn Inc,* David Wagner-*University of* California Berkeley, Chris Hall-*Princeton University*), *Rijndael* (Dr. Vincent Rijmen *Katholieke Universitei Leuven* dan Dr. Joan Daemen-*Proton World International*) dan *RC6* (RSA Amerika).

Setahun kemudian pada 2000, algoritma *Rijndael* terpilih sebagai algoritma kriptografi yang selain aman juga efisien dalam implementasinya dan dinobatkan sebagai AES. Nama *Rijndael* sendiri berasal dari gabungan nama penemunya.(Pabokory, dkk 2016:23).

Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah tebentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *chipertext.* Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu *round key* untuk setiap proses putaran. Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10) yaitu sebagai berikut :

1. *AddRoundKey* .
2. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey*.
3. *Final round* adalah proses untuk putaran terakhir yang meliputi *SubBytes, Shiftrows,* dan *AddRoundKey*. Sedangkan pada proses dekripsi AES 128, proses putaran juga dikerjakan sebanyak 10 kali (a=10).

2.2 Enkripsi Algoritma *AES*

Proses enkripsi pada algoritma *Advance Encryption Standard* terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes, ShiftRows, MixColumns,* dan *AddRound Key.* Pada awal pemrosesan enkripsi, input yang telah di-*copy*-kan ke dalam *state* akan mengalami transformasi byte *AddRoundKey*. Setelah itu, di *state* akan mengalami transformasi *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai *round function. Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumn.* Adapun proses enkripsi Algoritma AES dengan bit kunci 128 bit sebagai berikut:

1. Penambahan kunci putaran (*AddRoundKey*) adalah fungsi yang melakukan perhitungan XOR antara baris-baris matriks *plaintext* dengan baris-baris matriks kunci atau disebut juga sebagai tahap *initial round.*
2. Proses yang dilakukan pada setiap putaran adalah :
   a. Substitusi *byte* (*SubByte*) : substitusi *byte* dari matriks dengan menggunakan tabel S-box.
   b. Pergeseran baris *byte* (*ShiftRows*) : pergeseran ke kiri pada setiap baris-baris matriks.
   c. Pengacakan kolom (*MixColumns*): mengalikan setiap baris-baris matriks dengan tabel *MixColumns.*

d. Penambahan kunci putaran (*AddRoundKey*) : melakukan perhitungan XOR antara baris-baris matriks dengan kunci putaran.

3. Putaran terakhir
   a. Substitusi *byte* (*SubBytes*)
   b. Pergeseran baris *byte* (*ShiftRows*)
   c. Penambahan kunci putaran (*AddRoundKey*)

2.3 Dekripsi Algoritma *AES*

Transformasi *chiper* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *invers chiper* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *invers chiper* adalah *InvShiftRows, InvSubBytes, InvMixColumns,* dan *AddRoundKey.* Proses dekripsi Algoritma AES dengan bit kunci 128 bit sebagai berikut :

1. Penambahan kunci putaran (*AddRoundKey*) adalah fungsi yang melakukan perhitungan XOR antara baris-baris matriks *chipertext* dengan baris-baris matriks kunci.
2. Proses yang dilakukan pada setiap putaran adalah:
   a. *Invers-Pergeseran* baris *byte* (*Invers-Shiftrows*) : pergeseran ke kanan pada setiap baris-baris matriks.
   b. *Invers*-Substitusi *byte (Invers-SubBytes)* : substitusi *byte* pada setiap baris-baris matriks dengan tabel S-box.
   c. Penambahan kunci putaran *(AddRoundKey)* : melakukan perhitungan XOR antara baris-baris matriks dengan kunci putaran.
   d. *Invers*-Pengacakan kolom (*Invers-MixColumns*) : mengalikan setiap baris-baris matriks dengan tabel *MixColumns.*
3. Proses untuk putaran terakhir
   a. *Invers*-Pergesaran baris *byte (Invers-ShiftRows).*
   b. *Invers-Substitusi byte (Invers-SubBytes).*
   c. Penambahan kunci putaran (*AddRoundKey*).

3 ANALISA DAN HASIL

Analisa merupakan tahapan awal yang dilakukan untuk memecahkan sebuah permasalahan yang sedang terjadi pada sebuah kasus. Tahap analisa ini sangat penting karena proses analisis yang akurat akan menghasilkan sebuah aplikasi *web* yang dapat digunakan untuk kepala sub bagian umum. Mengenai permasalahan yang diambil dalam penelitian ini adalah bagaimana cara mengamankan data *file* dokumen yang berformat .docx dengan menggunakan algoritma kriptografi, yaitu AES *(Advance Encryption Standard).* Data yang akan diamankan adalah *file* arsip petikan SKKDD (Surat Keputusan Kepala Dinas Dishubsu) atau SKDD (Surat Keputusan Dinas Dishubsu) pada dinas perhubungan provinsi sumatera utara yang memiliki isi *file* terdiri dari nomor urut, nama, nip, golongan, informasi jabatan lama dan informasi jabatan baru yang berformat .docx. Berikut ini adalah gambar *file* arsip petikan surat keputusan kepala dinas perhubungan provinsi sumatera utara yang akan diamankan:

DINAS PERHUBUNGAN PROVINSI SUMATERA UTARA

PETIKAN

KEPUTUSAN KEPALA DINAS PERHUBUNGAN
PROVINSI SUMATERA UTARA
NOMOR : 824/ 622 /KP/PHB/2018

KEPALA DINAS PERHUBUNGAN PROVINSI SUMATERA UTARA

MEMBACA
MENIMBANG
MENGINGAT
MEMPERHATIKAN
- dst -

M E M U T U S K A N :

Menetapkan:

PERTAMA : Memindahkan Aparatur Sipil Negara yang namanya tersebut dalam lajur 2 (dua) dari tempat bekerja sebagai tersebut dalam lajur 5 (lima) ke tempat bekerja sebagai tersebut dalam lajur 6 (enam) dari daftar lampiran keputusan ini :

1. Nomor Urut : 122
2. N a m a : SUKADI ZAKARIA
3. N I P : 19650605 198712 1 001
4. Gol. Ruang : III/b
5. Jabatan Lama : Pengelola Terminal Seksi Pengawasan dan Pengendalian Operasional pada UPT Wasdalhub Medan Dishubsu
6. Jabatan Baru : **Pengawas Keselamatan Angkutan Seksi Perizinan dan Bimbingan Keselamatan pada UPT PSPP Langkat Dishubsu**
7. Pendidikan :

KEDUA : Keputusan ini mulai berlaku sejak tanggal **ditetapkan.**

KETIGA : Apabila dikemudian hari ternyata terdapat kekeliruan dalam keputusan ini akan diadakan perbaikan sebagaimana mestinya.

SALINAN : - dsbnya -

PETIKAN : Keputusan ini diberikan kepada yang berkepentingan untuk diketahui dan dipergunakan sebagaimana mestinya.

DITETAPKAN DI : M E D A N
PADA TANGGAL : 02 Juli 2018

Sesuai dengan aslinya,
SEKRETARIS
DINAS PERHUBUNGAN PROVSU

JUFFRI EDDY, SH, M.SP
PEMBINA TAMA MUDA
NIP 19610814 199003 1 003

KEPALA DINAS PERHUBUNGAN
PROVINSI SUMATERA UTARA

dto,

Drs. MOHAMMAD ZEIN, M.SI
PEMBINA UTAMA MADYA
NIP 19590118 198002 1 002

Gambar 3.1 Arsip Petikan Surat Keputusan Dinas Dishubsu

Arsip petikan adalah arsipan sebuah data ketentuan keputusan dari kepala dinas perhubungan provinsi sumatera uatara. Dimana arsip berikut sebagai data yang akan di jadikan data-data arsip pegawai dan disimpan sesuai nomor urut pada dokumen ini.

3.1 Proses Enkripsi

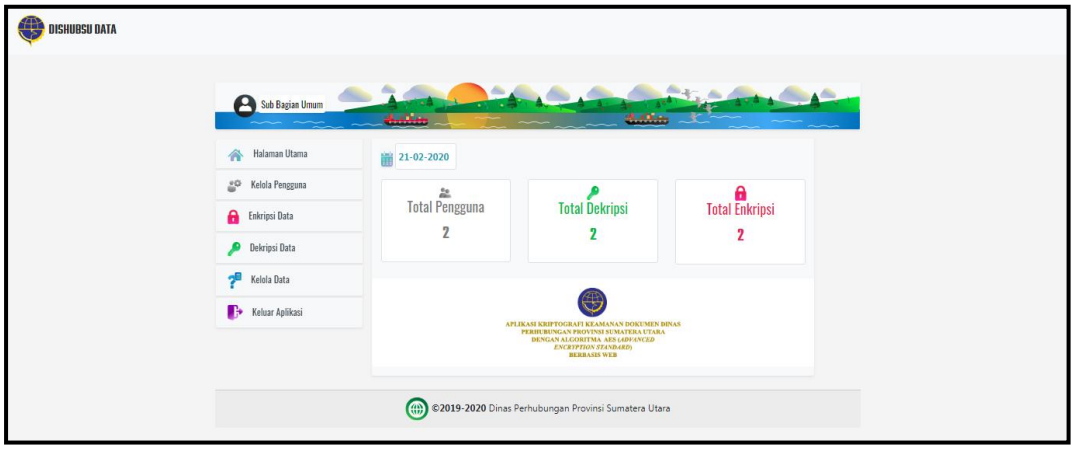
Pada aplikasi *web* ini terdapat empat *menu bar* yaitu halaman utama, kelola pengguna, enkripsi data, dekripsi data dan kelola data. Pada aplikasi ini ada 2 (dua) *menu* penting yaitu *form* enkripsi data dan *form* dekripsi data sebagai tahap pengujian aplikasi dalam pembahasan keamanan isi *file* dokumen dinas perhubungan provinsi sumatera utara. Adapun proses-proses dalam penggunaan aplikasi ini yaitu sebagai berikut:

1. *Form* Masuk Aplikasi

Form ini adalah tampilan *form* masuk aplikasi ke halaman utama aplikasi dengan cara mengisi nama pengguna dan kata sandi seperti pada gambar berikut:

Gambar 3.2 Tampilan *Form* Masuk Aplikasi

Sesudah masuk aplikasi pengguna langsung dihadapkan pada *menu* halaman utama aplikasi dan pengguna bisa melihat *informasi* dari pada halaman utama tentang total pengguna, total dekripsi dan total enkripsi supaya pengguna dapat mengetahui tentang jumlah pengguna, enkripsi dan dekripsi pada *file* di aplikasi berikut adalah tampilannya:

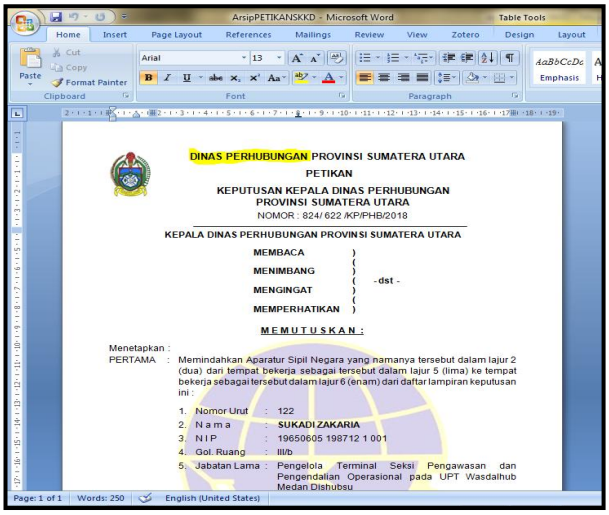


Gambar 3.3 Tampilan *Menu* Halaman Utama

2. Pengujian *Form* Enkripsi Data

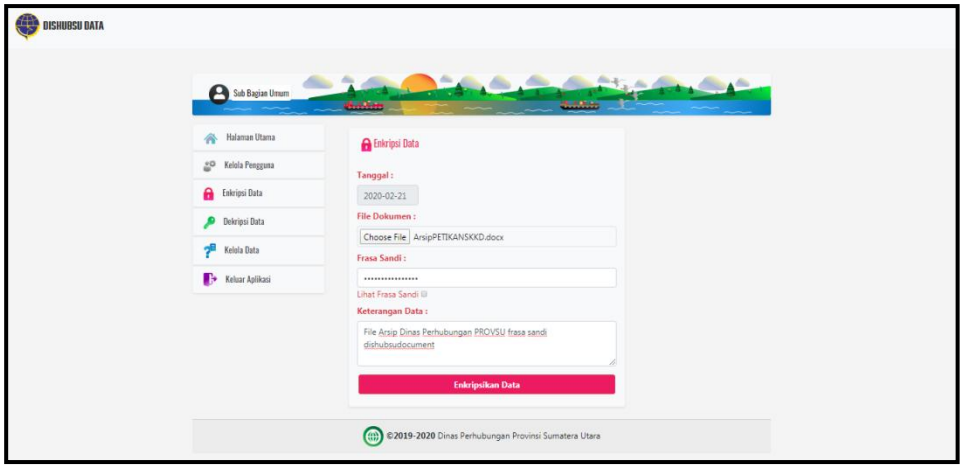
Enkripsi data ini terdapat *textbox* frasa sandi dan *button* enkripsikan data yang berguna untuk memproses enkripsi data pada *file* dokumen. Jika dienkripsikan maka hasilnya berupa *chipertext.* Berikut merupakan tahapan dari pengujian enkripsi data:

a. Memilih *file word* yang akan dienkripsi, adapun *file word* yang menjadi bahan pengujian adalah Surat Keputusan Dinas Perhubungan Provinsi Sumatera Utara atau Arsip PETIKAN Dinas Perhubungan Pronvisi Sumatera Utara dengan nama *file:* ArsipPETIKANSKDD.docx



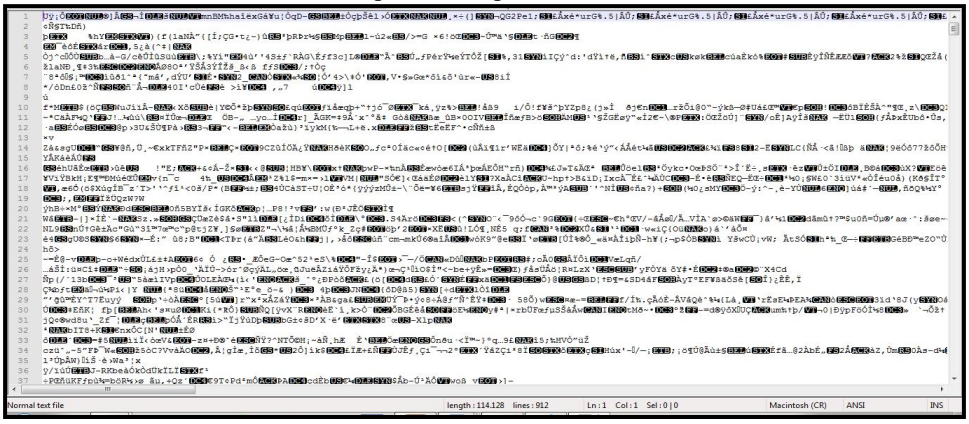
Gambar 3.4 Tampilan Isi Data *File* Sebelum Dienkripsi

b. Melakukan *input file* dokumen lalu mengisi *frasa sandi* enkripsi data dan membuat keterangan data pada *file* yang dienkripsikan setelah itu pilih *button* enkripsikan data.



Gambar 3.5 Tampilan *Input File* Dokumen Pada Enkripsi Data

Gambar 3.6 Tampilan Enkripsi *File* Dokumen Berhasil



Gambar 3.7 Tampilan *File* Dokumen Yang Sudah Dienkripsi

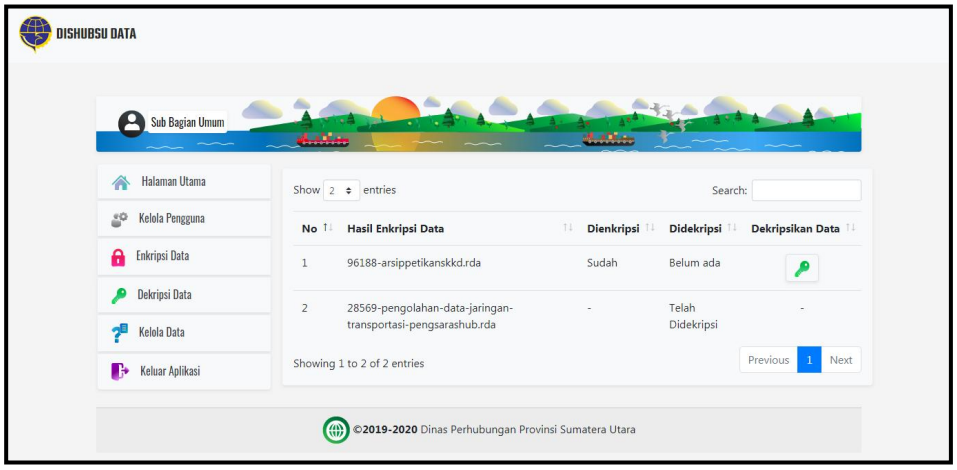
Pada gambar 3.7 merupakan tampilan *chipertext* hasil *output* dari analisa pada sebelumnya, yaitu:

Hasil *Chipertext Symbol*														
Å	Ž	Ñ	DC1	CAN		È	2	q	ñ	Ù	š	í	SOH	°	¿

3.2 Proses Dekripsi

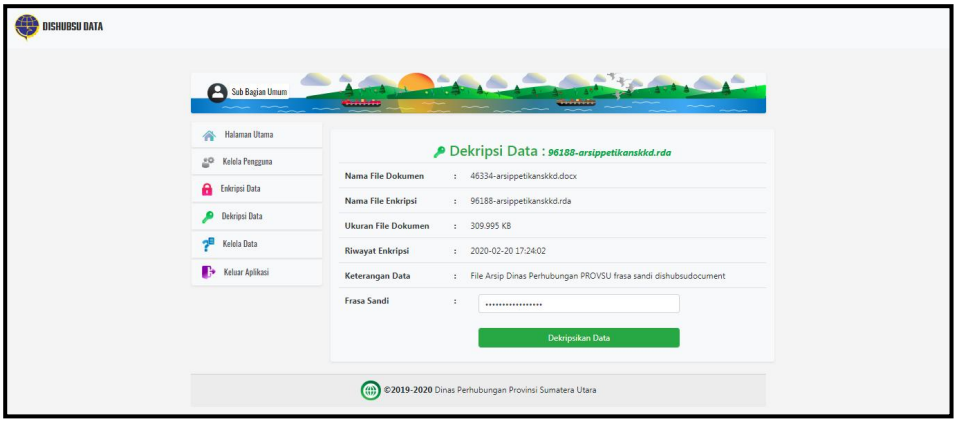
Dekripsi data ini terdapat komponen objek *textbox* frasa sandi dan *button* dekripsi data yang berguna untuk memproses dekripsi pada *file* dokumen yang hasilnya berupa *plaintext.* Berikut merupakan tahapan dari pengujian *form* dekripsi data:

a. Memilih daftar *file* yang akan didekripsi, yang ada pada daftar dengan nama *file* **96188-arsippetikanskkd.rda** yang sudah dienkripsi dan menekan *button symbol* dekripsikan data:



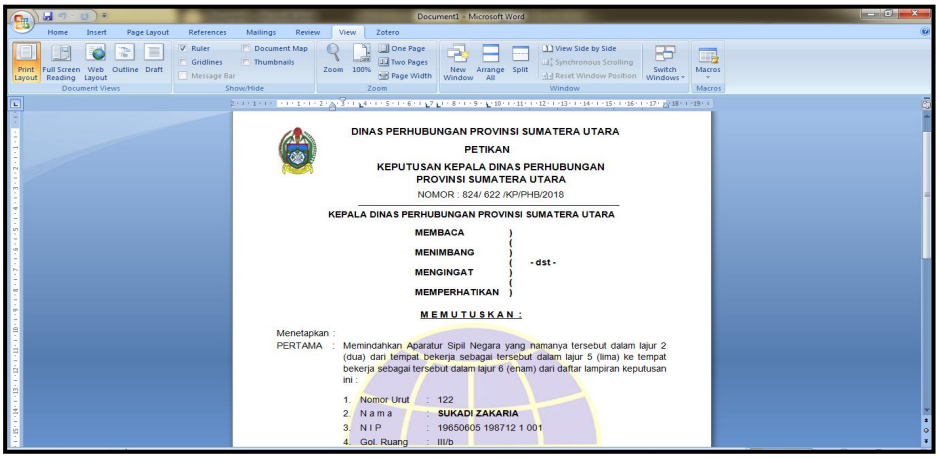
Gambar 3.8 Tampilan Daftar Dekripsi Data

b. Kemudian tampil *form* dekripsi data dengan mengetikkan frasa sandi yang dibuat pada saat menenkripsikan isi data *file* dokumen sebelumnya dan sistem akan menyamakan proses frasa sandi yang sama saat enkripsi dan dekripsi isi data *file* Arsip PETIKANSKDD.docx berikut tampilan pada saat mendekripsikan *file* **96188-arsippetikanskkd.rda**:



Gambar 4.9 Tampilan *Form* Dekripsi Data

Gambar 3.10 Tampilan Berhasil Mendekripsi *File*



Gambar 4.14 Tampilan *File* Berhasil Didekripsi

Maka dari hasil proses kesimpulan yang ada menunjukkan bahwa hasil *chipertext symbol* dan hasil *plaintext* adalah :

Hasil *Chipertext Symbol*														
Å	Ž	Ñ	DC1	CAN		È	2	q	ñ	Ù	š	í	SOH	°	¿

Hasil *Plaintext*															
D	**I**	**N**	**A**	**S**	**P**	**E**	**R**	**H**	**U**	**B**	**U**	**N**	**G**	**A**	**N**

5 . KESIMPULAN

Kesimpulan yang dapat diambil dalam proses pembuatan aplikasi kriptografi keamanan data dokumen dinas perhubungan provinsi sumatera utara dengan menggunakan algoritma AES *(Advanced Encryption Standard)* berbasis *web* adalah sebagai berikut:

1. Pengamanan *file* dokumen dengan teknik kriptografi dilakukan dengan cara menggunakan frasa sandi yang kunci keamanan data *file* dokumen hanya diketahui oleh pihak berwenang saja khususnya kepala sub bagian umum atau pengguna aplikasinya.
2. Dalam proses mengamankan isi data *file* dokumen dengan algoritma AES *(Advanced Encryption Standard)*, dimulai dengan melakukan ekspansi kunci, kemudian *AddRoundKey, SubBytes, ShiftRows* dan *MixColumns* kemudian *AddRoundKey* kembali. Sedangkan pada dekripsinya, terdapat perubahan urutan transformasi, yaitu *AddRoundKey, InvShiftRows, InvSubBytes, AddRoundKey* kemudian *InvMixColumns.*
3. Merancang dan mendesain sistem aplikasi kriptografi keamanan isi data pada *file* dokumen menggunakan algoritma AES *(Advanced Encryption Standard)* dilakukan dengan mengimplementasikan seluruh rancangan yang ada ke dalam bahasa pemrograman *web*.

UCAPAN TERIMA KASIH

Terima kasih kepada dosen pembimbing Bapak Badrul Anwar, S.E, S.Kom., M.Kom. dan Bapak Ismawardi Santoso, S.Kom., M.Kom. beserta pihak–pihak lainnya yang mendukung penyelesaian jurnal skripsi ini.

REFERENSI

[1] A.S Rosa dan M. Shalahuddin. 2016. Rekayasa Perangkat Lunak : Terstruktur dan Berorientasi Objek. Bandung. Informatika..

[2] Arief, M., dkk. 2015. Kriptografi RSA Pada Aplikasi *File Transfer Client-Server Based.* Ilmu Komputasi Universitas Telkom Bandung.

[3] Pabokory,. 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi *File* Dokumen, Dan *File* Dokumen Menggunakan Algoritma *Advanced Encryption Standard.*.

[4] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan : Mengenal Keamanan Jaringan, Dasar Matematika untuk Kriptografi, Kriptografi Klasik dan Modern, Implementasi dalam Bahasa Java Dll. Yogyakarta. C.V Andi Offset..

[5] Sholeh, dkk. 2013. Mengamankan Skrip Pada Bahasa Pemograman PHP Dengan Menggunakan Kriptografi *Base 64*.

[6] Soleh, Redi Taofik. 2007. VB 6.0 dan *Navicat MySQL*. Jakarta. PT.Flex Media Komputindo.

[7] Sumandri, 2017. Studi Model Algoritma Kriptografi Klasik dan Modern: Seminar Matematika dan Pendidikan Matematika.Universitas Negeri Yogyakarta

BIBLIOGRAFI PENULIS

Data Diri

Nama	: Vicky Ulfa Romyata Sembiring
Tempat/TanggalLahir	: Tanjung Morawa B, 25 April 1997
JenisKelamin	: Laki-Laki
Agama	: Islam
Pendidikan Terakhir	: Sekolah Menengah Atas
Kewarganegaraan	: Indonesia
E-mail	: vickyromyata@gmail.com

Badrul Anwar, S.E, S.Kom., M.Kom.

Ismawardi Santoso, S.Kom., M.Kom.