Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 54-60
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar

Imelda Asih Rohani Simbolon[1,*], Indra Gunawan[1], Ika Okta Kirana[1], Rafiqa Dewi[2], S. Solikhun[2]

[1]Program Studi Teknik Informatika, STIKOM Tunas Bangsa, Pematangsiantar, Indonesia
[2]Program Studi Manajemen Informatika, AMIK Tunas Bangsa, Pematangsiantar, Indonesia
Email: [1,*]imeldaasihrohanisimbolon@gmail.com

Abstrak−Data penduduk merupakan informasi tentang keberadaan seseorang didalam suatu negara. Masalah keamanan dan kerahasiaan data tersebut adalah hal yang sangat berpengaruh karena menyangkut tentang identitas seseorang, guna menghindari terjadinya pencurian dan manipulasi data maka perlu diterapkan sistem keamanan data. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan informasi seperti keabsahan data, integritas, serta autentifikasi data. Advanced Encryption Standard (AES) adalah salah satu metode yang digunakan dalam pengaman data/informasi. Pengimplementasian algoritma AES dalam pengamanan data penduduk Dinas Kependudukan dan Pencatatan Sipil menunjukkan bahwa metode tersebut dapat menghasilkan pesan yang tidak dapat dibaca maupun dimengerti oleh manusia (enkripsi) dan menghasilkan pesan yang sama seperti plaintext awal yang di-imput-kan (dekripsi).

Kata Kunci: Keamanan, AES, Enkripsi, Dekripsi, Data Penduduk

Abstract−Population data is information about the existence of someone in a country. The data can be accepted as validity through management in one of the government agencies. The issue of security and confidentiality of the data is something that is very important because it concerns the identity of a person, in order to avoid theft and manipulation of data it is necessary to apply a data security system. Cryptography is the study of mathematical techniques related to aspects of data and information security such as data validity, integrity, and data authentication. The Advanced Encryption Standard (AES) is one method used in data / information safeguards. The implementation of the AES algorithm in securing population data of the Population and Civil Registration Service shows that the method can produce messages that cannot be read or understood by humans (encryption) and produce the same message as the initial plaintext that was imputed (decryption).

Keywords: Security, AES, Encryption, Decryption, Population

1. PENDAHULUAN

Seiring dengan kemajuan ilmu pengetahuan dan teknologi saat ini, teknologi informasi selalu beriringan dengan segala aktivitas di dalam kehidupan manusia, karena kemampuan komputer untuk mengolah dan menyimpan data melebihi kecepatan manusia. Dengan pesatnya kemajauan telekomunikasi dan komputer itu memungkinkan penyimpanan dilakukan secara digital oleh pengguna [1]. Penggunaan teknologi informasi, media, dan komunikasi dapatmempengaruhi pola hidup maasyarakat seiring dengan perkembangan zaman secara menyeluruh.. Kondisi ini mengakibatkan maraknya terjadi penipuan melalui berbagai media komunikasi. Hal ini biasa dilakukan oleh kelompok atau pihak-pihak yang tidak bertanggung jawab untuk mengambil keuntungan dari masyarakat awam yang tidak paham atas ketentuan hukum yang berlaku.

Dinas Kependudukan dan Pencatatan Sipil Pematangsiantar (DISDUKCAPIL) bergerak di bidang pelayanan informasi dan pengurusan data kependudukan, dimana instansi tersebut menggunakan komputer dalam penerapan kegiatan pelayanan jasa. Dari hasil pengamatan penulis dinas tersebut belum menerapkan sistem keamanan untuk data penduduk. Komputer yang digunakan dapat diakses oleh siapapun sehingga sangat beresiko apabila ada orang yang tidak bertangung jawab mengakses informasi yang sensitif dan berharga tersebut. Kemungkinan lainnya adalah unsur yang terdapat di dalamnya dapat berganti sehingga dapat mengakibatkan perubahan data penduduk dan juga bisa disalahgunakan untuk kepentingan yang tidak baik bagi si pemilik data, selain itu data hilang dan akan menyebabkan kerugian finansial yang besar. Untuk menangani terjadinya pencurian, penyalahgunaan dan kerusakan data maka, penulis menggunakan algoritma kriptografi AES dari sekian banyak algoritma kriptografi untuk proses enkripsi dan deskripsi data. Kriptografi merupakan sisi penting yang saling berkaitan dari sistem keamanan. Advanced Encryption Standard (AES) yang merupakan metode kriptografi yang bisa dimanfaatkan untuk menyelamatkan data dalam berbagai aplikasi [2]. Algoritma AES adalah blok chipertext simetrik yang digunakan untuk mengenkripsi (encipher) dan mendekripsi (decipher) informasi. DES (Data Encryption Standard) telah digantikan oleh AES (Advanced Encryption Standard) karena keamanan AES sudah lebih baik dibandingkan dengan metode DES.

Pada penelitan sebelumnya [3] melakukan penelitian dalam kompresi data teks. Dimana hasil penelitian membuktikan penggunaan algoritma AES 128-bit mampu menyandikan isi header dari file terkompresi sehingga dapat mengamankan file tersebut. Sementara rasio hasil kompresi pada Kompresi yang mengimplementasikan metode Kriptografi AES menjadi sistem terpadu adalah sebesar 41,80% untuk file uji *.txt dan 25,09% untuk file uji *.htm. Selanjutnya [4] melakukan penelitian dalam pengamanan data untuk pesan teks yang berupa isi data dokumen atau file dan data dokumen menggunakan algoritma AES. AES adalah algoritma kriptografi untuk mengamakan data dimana algoritmanya adalah blokchipertext simetrik yang dapat mengenkripsi dan mendekripsi informasi. Hasil dari penelitian yaitu pesan teks dapat dienkripsi oleh pengguna dan disimpan

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 54-60
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

menjadi sebuah file dokumen dan file tersebut dienkripsi lagi dan hasil enkripsi file tersebut dikompresi dan disembunyikan pada sebuah file citra (gambar). Pengamanan dan penyandian yang berlapis-lapis dilakukan agar keamanan data informasi dapat terjaga.

2. METODOLOGI PENELITIAN

2.1 Penerapan

Penerapan merupakan tahap pengimplementasian ide, rencana kebijakan atau inovasi pada suatu tindakan praktis, sehingga memberi dampak baik perubahan pengetahuan, keterampilan maupun nilai dan sikap [5].

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani, *Crypto* berarti rahasia *(secret)* dan *Graphia* berarti tulisan *(writing).* Adapun pengertian kriftografi menurut [6] adalah ilmu yang mempelajari teknik-teknik matematika yang saling berkaitan dengan aspek keamanan data dan informasi seperti autentifikasi data, keabsahan data, serta integritas data.Menurut [7] kriptografi memiliki 4 tujuan yaitu:

a. Kerahasiaan *(confidentiality)*, Adalah layanan yang diperuntukkan untuk kepentingan dalam penjagaan keamanan kerahasiaan pesan agar pihak yang tidak berkepintingan tidak dapat memahami apa isi dari pesan tersebut.
b. Integritas data *(data integrity)*, adalah layanan yang menjamin bahwa tidak terjadi manipulasi pesan atau merubah isi pesan sehingga isi pesan masih asli dan terjaga kerahasiaannya selama proses pengiriman.
c. Otentikasi *(authentication)*, adalah layanan yang berhubungan dengan melakukan identifikasi tentang kebenaran sumber pesan, baik mengidentifikasi kebenaran pihak - pihak yang melakukan komunikasi.
d. Nir penyangkalan *(non-repudiation)*, adalah layanan yang mencegah penyangkalan terjadi saat proses pengiriman data.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi [8]:

a. Pesan *(Plaintext dan Ciphertext)* : Pesan *(message)* merupakan data, isi pesan atau informasi yang mampu dibaca dan dipahami artinya. *Plaintext* (P) merupakan pesan yang berisi data asli atau informasi yang akan dikirimkan. *Ciphertext* (C) merupakan pesan yang telah berubah arti dari pesan asli atau pesan terenkrip (tersandi) yang merupakan hasil enkripsi.
b. Pengirim dan Penerima : Pengirim (*sender*) adalah seseorang atau pihak yang akan mengirimkan pesan kepada pihak yang dituju. Penerima (*receiver*) adalah seseorang yang menerima pesan yang telah dikirim oleh si pengirim. Pengirim/penerima adalah sesuatu yang dapat mengirimkan pesan melalui orang, atau menggunakan mesin (komputer), kartu kredit dan sebagainya.
c. Penyadap *(eavesdropper)* adalah orang yang ingin mencoba membobol, meretas atau menangkap pesan selama proses pengiriman.
d. Kriptanalisis dan Kriptologi : Kriptanalisis *(cryptanalysis)* merupakan ilmu dan seni yang akan digunakan dalam memecahkan chiperteks menjadi plainteks tanpa kita harus mengetahui kuncinya. Dan untuk pelakunya biasa disebut dengan kriptanalis.. Kriptologi *(cryptology)* Merupakan pelajaran mengenai kriptografi dan pemecah chiperteks (kriptanalis).
e. Enkripsi (E) adalah proses pengubahan *plaintext* menjadi *ciphertext*. Dekripsi (D) Merupakan proses pengubahan hasil dari proses enkripsi ataupun chiperteks menjadi plainteks sehingga kembali ke data awal/asli.
f. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

2.3 Advanced Encryption Standard (AES)

Karena *DES* dianggap sudah tidak aman lagi, Agensi Departemen Perdagangan AS, *National Institute of Standard and Technology* yang sebelum tahun 1988 juga dikenal sebagai *National Bureau of Standard*, mengusulkan kepada Pemerintah Federal AS untuk merancang sebuah standard kriptografi baru. Untuk menghindari kontroversi mengenai standard yang baru tersebut, sebagaimana terjadi pada pembuatan *DES*, dimana waktu itu *NSA* yang berperan sebagai penilai kekuatan algoritma, maka *NIST* mengadakan sayembara terbuka untuk membuat standard algoritma kriptografi yang baru sebagai pengganti *DES*. Algoritma *AES (Advanced Encryption Standard)* ditemukan oleh Vincent Rijnmen dan Joan Daeman dar Belgia. Evaluasi terhadap *Rijndael* dijelaskan sebagai berikut :

a. Belum ada jenis serangan yang telah diketahui yang dapat memecahkan algoritma *Rijndael*.
b. Algoritma ini memakai *S-Box nonlinier*.
c. *Rijndael* tidak memakan banyak sumber daya komputasi. Kecepatan antara dekripsi lebih lama daripadan enkripsinya.

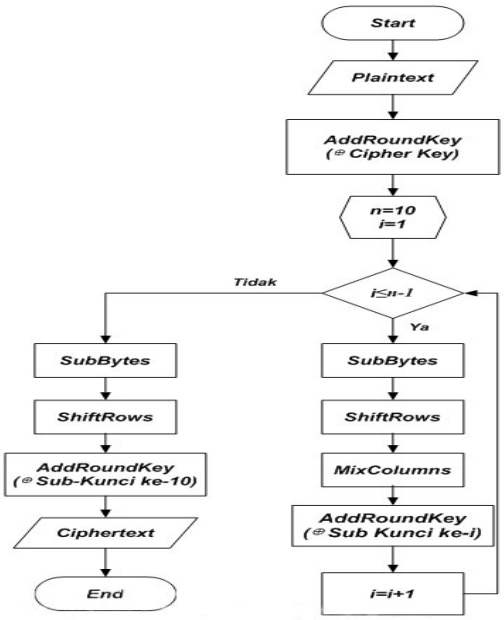
Menurut [9] tahap-tahap metode *Advanced Encryption Standard (AES)* yang umum pada blok dan panjang kunci 128 bit adalah sebagai berikut:

a. *AddRoundKey*. yang merupakan *initial round* yang melakukan *XOR* antara plaintext dengan *chipper key*.
b. Putaran sebanyak 10 kali meliputi proses berikut ini.
    1. *SubBytes*. Proses ini mensubstitusi *byte*.

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 54-60
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

2. *ShiftRows*. Proses ini melakukan pergeseran 1 kali ke kiri untuk baris 2 dari *state*, pergeseran 2 kali ke kiri untuk baris 3 dari *state*, dan pergeseran 3 kali ke kiri untuk baris 4 dari *state*.
3. *MixColumns*. Proses ini mengalikan kolom state satu persatu dengan modular *multiplication*.
4. *AddRoundKey*. Proses ini melakukan *XOR* antara *state* dengan *round key*.

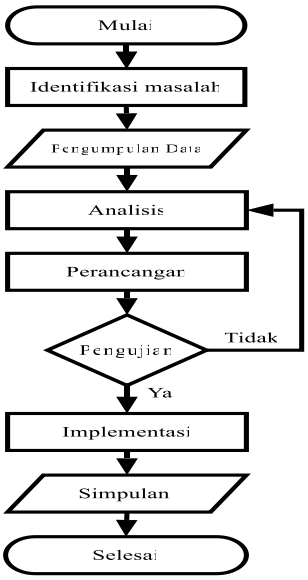
c. Proses terakhir merupakan putaran terakhir atau *final* round meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey*.



Gambar 1. Logo Jurnal BITS

2.4 Kerangka Kerja Penelitian

Kerangka kerja yang digunakan penulis dalam menyelesaikan permasalahan ini yaitu :



Gambar 2. Kerangka Kerja Penelitian

Dari gambar 2, langkah – langkah kerja penelitian dapat dijelaskan sebagai berikut :

a. Identifikasi Masalah
b. Seringnya terjadi kasus manipulasi data akan menyebabkan kerugian bagi si pemilik data. Pada tahap ini perlu dilakukan pengamatan secara langsung terhadap instansi yang bersangkutan khususnya masalah keamanan data.
c. Pengumpulan Data
   Pada tahap ini data yang akan diamankan diambil dari Dinas Kependudukan dan Pencatatan Sipil Kota Pematangsiantar dengan menggunakan metode pengumpulan data melalui wawancara, observasi dan studi literatur yang diperlukan dalam membantu memecahkan permasalahan.
d. Analisis

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 54-60
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Pada tahap ini terlebih dahulu dilakukan analisis terhadap algoritma *Advanced Encryption Standard (AES)* sehingga dapat di implementasikan pada keamanan data penduduk.

e. Perancangan
Pada tahap ini akan menjelaskan apa yang akan dirancang oleh penulis dengan menggunakan aplikasi *Netbeans* dangan bahasa pemograman *JAVA*.

f. Pengujian
Pada tahap ini dilakukan pengujian aplikasi keamanan data penduduk.

g. Implementasi
Pada tahapan ini penulisi melakukan beberapa tahapan implementasi diantaranya persiapan menginstal *netbeans*, dan pembuatan program dengan membangun aplikasi sesuai pada fitur yang ditentukan.

h. Simpulan
Pada tahap ini dilakukan penarikan kesimpulan akhir yang diperoleh setelah melakukan tahap anlisis, perancangan, pengujian dan implementasi apakah aplikasi yang dibuat dengan menerapkan algoritma *AES*.

2.5 Data Penduduk

Penduduk adalah orang-orang yang bertempat tinggal di sekitar wilayah Republik Indonesia dengan rentang waktu enam bulan atau lebih atau orang yang bertujuan menetap di dearah indonesia menjadi masyarat Indonesia mskipun kurang dalam kurun waktu dari enam bulan [10]. Setiap penduduk memiliki data kependudukannya untuk menyatakan bahwa ia adalah penduduk di wilayah domisilinya.

2.6 Java

Java adalah sebuah bahasa pemrograman yang diciptakan oleh James Gosling, seorang developer dari *Sun Microsystem* pada tahun 1991. Selanjutnya *Java* dikembangkan *Sun Microsystem* dan banyak digunakan untuk menciptakan *Executable Content* yang dapat didistribusikan melalui *network*. *Java* adalah bahasa pemrograman *Object-Oriented* dengan unsur-unsur seperti bahasa C++ dan bahasa-bahasa lainnya yang memiliki libraries yang cocok untuk lingkungan *internet*. *Java* adalah bahasa berorientasi objek yang dapat digunakan untuk pengembangan aplikasi mandiri, aplikasi berbasis *internet*, serta aplikasi untuk perangkat perangkat cerdas yang dapat berkomunikasi lewat internet atau jaringan komunikasi [11].

2.7 Netbeans

Netbeans merupakan salah satu *IDE* yang dikembangkan dengan bahasa pemrograman *java*. *Netbeans* mempunyai lingkup pemrograman *IAVA* terintergrasi dalam suatu perangkat lunak yang didalamnya menyediakan pembangunan pemrograman *GUI*, *text editor*, *compiler*, dan *interpreter*. *Netbeans* merupakan salah satu *IDE* yang dikembangkan dengan bahasa pemrograman *java*. *Netbeans* mempunyai lingkup pemrograman *JAVA* terintergrasi dalam suatu perangkat lunak yang didalamnya menyediakan pembangunan pemrograman *GUI*, *text editor*, *compiler*, dan *interpreter* [12].

2.8 Analisis Data

Analisis data adalah suatu proses atau langkah-langkah dimana semua tindakan analisisnya dilakukan terhadap data apa saja yang akan diolah dalam prospek atau tahapan sebuah rancangan. Dalam kasus ini data yang akan dienkripsi pada aplikasi kriptografi ini adalah file dengan ekstensi *.doc*, *.xls*, *.ppt*, *.pdf*, *.jpg* dan *.png*.

3. HASIL DAN PEMBAHASAN

Aplikasi hanya dapat melalukan Enkripsi dan Dekripsi *file* yang dapat kitaakses pada menu utama seperti gambar berikut.

Gambar 3. Tampilan Menu utama

Dapat dilihat dari tampilan menu utama terdapat pilihan dua menu utama yaitu enkripsi *file* dan dekripsi *file*. Sedangkan pada menu profil hanya terdapat pilihan *log out*.

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 54-60
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Gambar 4. Tampilan Menu Log Out

Tahapan enkripsi *file* dengan aplikasi kriptografi ini adalah sebagai berikut :

a. Lakukan enkripsi *file*.
b. Pilih *file* yang akan dienkripsi.
c. Masukkan *password* dan konfirmasi *password*. *Password* yang digunakan sesuai dengan yang diinginkan oleh si pemakai ataupun *user*.
d. Program akan melakukan proses enkripsi *file* dan kemudian menuliskan *file output*. *File* hasil enkripsi akan tersimpan secara langsung di direktori yang sama dan menggantikan *file* asli.

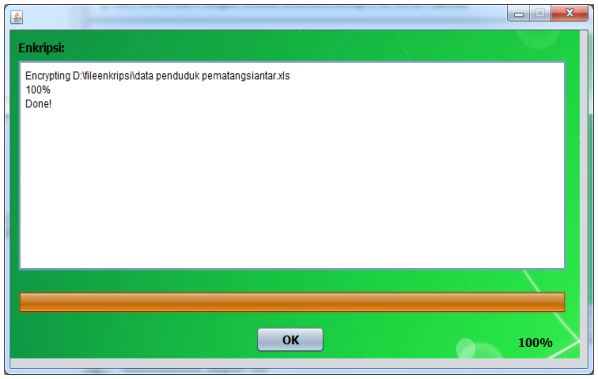
Sebelum menginkripsi *file* maka *user* terlebih dahulu memasukkan kunci untuk enkripsi *file*. Adapun kunci yang digunakan untuk enkripsi harus sama dengan kunci dekripsi yang memiliki sebanyak 16 karakter dimana untuk panjang 128 bit berarti 16 *byte* (16 karakter). Lalu klik proses untuk melanjutkan proses enkripsi *file*.

Gambar 5. Tampilan Pengisian Kunci Enkripsi

Apabila melanggar aturan tersebut program juga akan mengeluarkan pesan, dimana kunci kurang dari 16 karakter.

Gambar 6. Tampilan *Error* Kunci

Setelah proses enkripsi selesai maka akan muncul notifikasi menu yang menyatakan enkripsi telah berhasil.



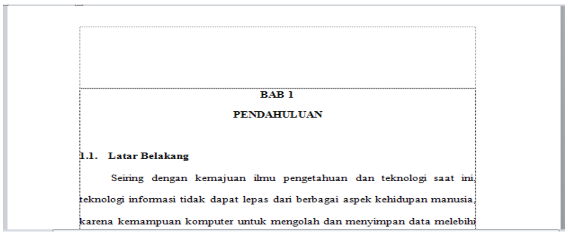
Gambar 7. Tampilan Enkripsi Berhasil

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 54-60
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

3.1 Pengujian Sistem

Proses enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext* yang bertujuan untuk mengamankan data atau isi pesan agar tidak dapat dipahami oleh pihak lain sehingga, perlu dilakukan analisis isi *file* untuk melihat apakah *file* yang akan dienkripsi dapat terjaga kerahasiaannya. Berikut ini contoh analisis pada beberapa *file* dengan ekstensi berbeda.

a. *File* Document *(.doc/.docx)*
   1. *File* Asli (pendahuluan.*docx*)



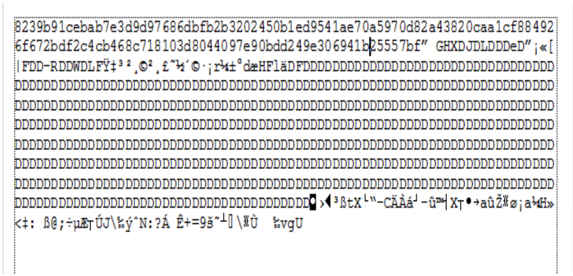
BAB 1
PENDAHULUAN

1.1. Latar Belakang

Seiring dengan kemajuan ilmu pengetahuan dan teknologi saat ini, teknologi informasi tidak dapat lepas dari berbagai aspek kehidupan manusia, karena kemampuan komputer untuk mengolah dan menyimpan data melebihi

Gambar 8. *File* Pendahuluan.*docx*

   2. *File* Hasil Enkripsi *(Abstrak.docx.enc)*



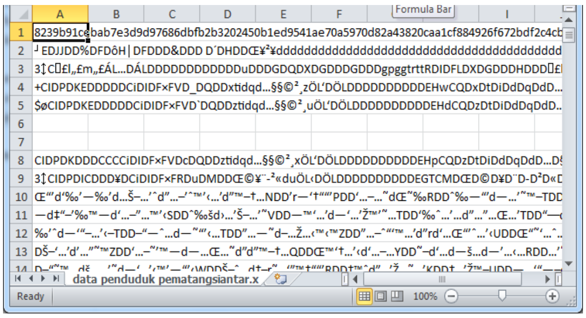
Gambar 9. File Enkripsi Pendahuluan.*docx*

b. File Excel *(.xls/.xlsx)*
   1. File Asli (Data Penduduk Pematangsiantar..*xlsx*)

	A	B	C
1	NAMA_LENGKAP	JENIS_KLMIN	TMPT_LHR
2	FRENGKY REGEND ROY PANGGABEAN	1	PEMATANGSIANTAR
3	WALMAN MULYADI HUTAPEA	1	LAGUBOTI
4	LASTIAR ENDANG SIMANJUNTAK	2	PEMATANG SIANTAR
5	ANDREW IMMANUEL JOGI HUTAPEA	1	PEMATANG SIANTAR
6	LAURA NAOMI ANGGI NAINGGOLAN	2	PEMATANGSIANTAR
7	SITOR OPITO NAINGGOLAN	2	PEMATANGSIANTAR
8	NY NARUMONDANG TAMPUBOLON	2	BALATA
9	BINTANG HANAEFLIN SILALAHI	2	PEMATANGSIANTAR
10	ANDREAS SIMBOLON	1	PEMATANGSIANTAR
11	RAFKA AL DAMA	1	PEMATANGSIANTAR
12	RAMLINUS SITORUS	1	PEMATANGSIANTAR
13	HELEN REPINA SIMANJUNTAK	2	PEMATANGSIANTAR
14	ROMIANA PASKA SIBARANI	2	PEMATANGSIANTAR
15	HERMAN TOGAR PEBRIO MUNTHE	1	P.SIANTAR
16	ANDAR DUABEL SIDABUTAR	1	PEMATANG SIANTAR

Gambar 10. File DataPenduduk Pematangsiantar.*xlsx*

c. *File* Hasil Enkripsi (SSR PER 01 - 03 OKT 2018.*xlsx)*



Gambar 11. Gambar File Enkripsi Dta Penduduk Pematangsiantar.*xlsx*

Selain kedua *file* di atas, penulis juga melakukan pengujian pada *file- file* lain dengan ekstensi berbeda seperti *.ppt, .pdf, .jpg* dan *.png.* Hasil pengujian menunjukkan bahwa setelah dilakukan proses enkripsi, *file-file* tersebut tidak dapat dibaca dan dimengerti maknanya dan setelah dilakukan proses dekripsi maka *file-file* tersebut dapat dibaca dan dimengerti kembali maknanya

4. KESIMPULAN

Setelah selesai dilakukan analisis, perancangan serta implementasi menggunakan algoritma *Advance Encryption Standard (AES)* dapat ditarik kesimpulan sebagai berikut:

1. Dengan adanya sistem keamanan data penduduk di DISDUKCAPIL Kota Pematangsiantar dapat terbantu dalam mengamankan data-data yang bersifat rahasia di instansi DISDUKCAPIL.
2. Hasil enkripsi merupakan sekumpulan kombinasi karakter yang tidak dapat dimengerti oleh manusia.
3. Untuk hasil enkripsi akan selalu sama dengan hasil dekripsi dengan menggunakan kunci yang sama.
4. Dari implementasi Algoritma kriptografi *AES* dapat mengamankan *file* penduduk dengan jenis ekstensi seperti : *.doc, .xls, .ppt, .pdf, .jpg* dan *.png.*

REFERENCES

[1] A. K. Prastyo, "Pengamanan Data Dengan Metode Advanced Encryption Standard dan Metode List Significant Bit," 2014.
[2] E. Budi, H. Sibarani, P. M. Zarlis, and R. W. Sembiring, "Analisis Kripto Sistem Algoritma AES dan Elliptic Curve Cryptography (ECC) Untuk Keamanan Data," *Nasional Informatika Dan Teknologi Jaringan*, vol. 1, no. 2, pp. 106–112, 2017.
[3] S. H. Putra, E. Santoso, and L. Muflikhah, "Implementasi Algoritma Kriptografi Advanced Encryption Standard (AES) Pada Kompresi Data Teks," *Jurnal Ilmu Komputer*, pp. 1–14, 2013.
[4] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Jurnal Informatika Mulawarman*, vol. 10, no. 1, pp. 20–31, 2015.
[5] A. Wanto, A. P. Windarto, D. Hartama, and I. Parlina, "Use of Binary Sigmoid Function And Linear Identity In Artificial Neural Networks For Forecasting Population Density," *International Journal Of Information System & Technology*, vol. 1, no. 1, pp. 43–54, 2017.
[6] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Matematika UNISBA*, vol. 15, no. 1, pp. 7–14, 2016.
[7] M. K. Harahap, "Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks," *Jurnal & Penelitian Teknik Iformatika*, vol. 1, no. April 2017, pp. 58–62, 2019.
[8] A. Farisi, "Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone," *Jatisi*, vol. 4, no. 2, pp. 199–208, 2018.
[9] S. Wibowo, F. E. Nilawati, and Suharnawi, "Implementasi Enkripsi Dekripsi Algoritma Affine Chiper Berbasis Android," *Techno*, vol. 13, no. 4, pp. 215–221, 2014.
[10] M. Mujito and A. Bagus Susilo, "Aplikasi Kriptografi File Menggunakan Metode Blowfish dan Metode Base64 pada Dinas Kependudukan dan Pencatatan Sipil Kota Tangerang Selatan," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 5, no. 1, pp. 54–60, 2016.
[11] H. N. Lengkong, A. A. E. Sinsuw, and A. S. M. Lumenta, "Perancangan Penunjuk Rute Pada Kendaraan Pribadi Menggunakan Aplikasi Mobile GIS Berbasis Android Yang Terintegrasi Pada Google Maps," *E-Kournal Teknik Elektro dan Komputer*, pp. 18–25, 2015.
[12] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *Jurnal Format*, vol. 6, no. 2, pp. 87–105, 2016.