

# IMPLEMENTASI KRIPTOGRAFI AES-128 DALAM APLIKASI PENGAMANAN DATA UNTUK MENJAGA KERAHASIAAN DI SMK PGRI 15 JAKARTA

Denise Fatthurrahman<sup>1\*</sup>, Purwanto<sup>2</sup>, Gunawan Pria Utama<sup>3</sup>, Painem<sup>4</sup>

<sup>1,2,3,4</sup>Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: <sup>1\*</sup>1911500203@student.budiluhur.ac.id, <sup>2</sup>purwanto@budiluhur.ac.id, <sup>3</sup>gunawan.priautama@budiluhur.ac.id,  
<sup>4</sup>painem@budiluhur.ac.id  
(\* : corresponding author)

**Abstrak**-Seiring perkembangan teknologi, data SMK PGRI 15 Jakarta yang tersimpan harus terjamin keamanannya dari ancaman dan manipulasi. File yang bersifat internal dan tidak semua boleh dipublikasi, perlu diamankan dan dijaga ke rahasiannya. Untuk mengatisifasi kebocoran data tersebut, maka kriptografi adalah salah satu pilihan yang dapat digunakan. Algoritme kriptografi yang dipilih adalah AES-128 (*Advanced Encryption Standard-128*). Algoritme AES dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Panjang kunci akan mempengaruhi jumlah *round* (perputaran), dan waktu saat melakukan enkripsi. Alasan AES-128 terpilih karena AES-128 memiliki panjang kunci dan *round* yang lebih sedikit untuk mempercepat waktu saat melakukan enkripsi. Aplikasi ini dibangun dengan bahasa pemrograman PHP berbasis web dan database menggunakan MySQL. Beberapa data yang kemudian bisa dienkripsi dan didekripsi yaitu dengan tipe file \*.doc, \*.xls, \*.ppt, \*.txt, \*.docx, \*.xlsx, \*.pptx, \*.png, \*.jpg, \*.pdf. Hasil penelitian menunjukkan bahwa aplikasi ini dapat mengamankan dan menjaga kerahasiaan data dan informasi pada SMK PGRI 15 Jakarta dari terjadinya pencurian dan manipulasi data oleh pihak yang tidak berkepentingan.

**Kata Kunci:** Keamanan, Kriptografi, AES-128, Enkripsi, Dekripsi

## IMPLEMENTATION OF AES-128 CRYPTOGRAPHY IN DATA SECURITY APPLICATIONS TO MAINTAIN CONFIDENTIALITY AT SMK PGRI 15 JAKARTA

**Abstract**-Along with the development of technology, the data stored at SMK PGRI 15 Jakarta must be secured from threats and manipulation. Files that are internal and not all can be published, need to be secured and kept confidential. To prevent data leakage, cryptography is one option that can be used. The cryptographic algorithm chosen is AES-128 (*Advanced Encryption Standard-128*). The AES algorithm can encrypt and decrypt data with varying key lengths, namely 128 bits, 192 bits, and 256 bits. The key length will affect the number of rounds, and the time when performing encryption. The reason AES-128 was chosen is because it has a lower key length and fewer rounds to speed up the encryption time. This application is built with a web-based PHP programming language and a database using MySQL. Some data that can then be encrypted and decrypted are with file types \*.doc, \*.xls, \*.ppt, \*.txt, \*.docx, \*.xlsx, \*.pptx, \*.png, \*.jpg, \*.pdf. The results showed that this application can secure and maintain the confidentiality of data and information at SMK PGRI 15 Jakarta from theft and data manipulation by unauthorised parties.

**Keywords:** Security, Cryptography, AES-128, Encryption, Decryption

## 1. PENDAHULUAN

Perkembangan teknologi informasi semakin pesat, khususnya di bidang teknologi informasi. Sehingga memberikan dampak positif, dan dampak negatif dalam perkembangan teknologi informasi penyediaan data. Masalah keamanan dan kerahasiaan dari sebuah informasi, dan data merupakan suatu aspek penting. Informasi dan data merupakan bagian yang penting dari sebuah instansi maupun individu[2].

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. “*Crypto*” yang artinya “*secret*” (rahasia) dan “*graphy*” yang artinya “*writing*” (tulisan). Jadi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang akan dikirim ke penerima sehingga data atau pesan tersebut aman dan tidak di ketahui oleh pihak ketiga. Data atau pesan yang di kirim akan berubah menjadi kode-kode yang tidak dapat dipahami oleh pihak ketiga[1].

Ilmu kriptografi yaitu salah satu fasilitas untuk menterjemahkan pesan jelas (*plainteks*) menjadi pesan yang telah terkunci (*cipherteks*). Adapun langkah untuk melakukan suatu terjemahan disebut enkripsi (*encryption*)

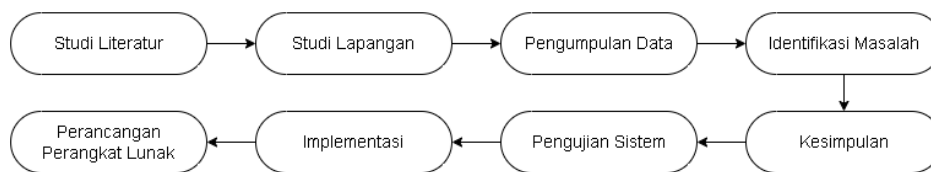
menterjemahkan cipherteks menjadi plainteks disebut dengan dekripsi (*decryption*) proses enkripsi dan dekripsi menggunakan kunci kriptografi[5].

Algoritme kriptografi yang digunakan saat mengenkripsi data atau informasi apa pun yang terkait dengan masalah ini adalah *Advanced Encryption Standard*(AES). Algoritma AES adalah algoritme enkripsi blok yang menggunakan teknik substitusi, mutasi dan putaran ganda dari setiap *blok* selama enkripsi dan dekripsi. Pada penelitian ini, proses enkripsi dan dekripsi menggunakan algoritma enkripsi AES-128 untuk melindungi data. Algoritme AES memiliki panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Dari ketiga kunci tersebut mempunyai jumlah round (perputaran) yang berbeda-beda[8].

Pada proses enkripsi, ada 4 jenis transformasi *byte* pada algoritme AES, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. *SubBytes* adalah transformasi *byte* dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel substitusi (S-Box). Transformasi *ShiftRows* pada dasarnya merupakan proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). *MixColumns* melakukan operasi pada setiap elemen yang ada didalam satu kolom pada state. *AddRoundKey* merupakan sebuah round key ditambahkan pada state dengan operasi XOR[6].

## 2. METODE PENELITIAN

Metode yang digunakan pada topik ini adalah metode waterfall yang akan digunakan sebagai pedoman dalam pelaksanaan penelitian yang dibuat, sehingga hasil yang dicapai tidak ada penyimpangan dari tujuan yang sudah dilakukan sehingga hasil dari penelitian dapat lebih baik.



Gambar 1. Flowchart penelitian

### 2.1 Pengumpulan Data

Pada tahap pengumpulan data ini dilakukan untuk mengumpulkan data yang dibutuhkan untuk perancangan sistem, adapun beberapa pendekatan yang dilakukan adalah sebagai berikut:

- Wawancara Dilakukan tanya jawan kepada pihak-pihak yang terkait. Untuk mendapatkan informasi tentang kebutuhan untuk menjalankan sistem pengamanan file dokumen
- Observasi Mengumpulkan data dan mempelajari proses yang terjadi dengan cara pengamatan secara langsung di SMK PGRI 15 Jakarta yang nantinya digunakan sebagai masukan laporan penelitian
- Studi Pustaka Dilakukan dengan cara membaca *e-book* dan jurnal serta referensi lainnya yang berkaitan dengan teori kriptografi, teori pengamanan file, teori dari metode AES dan teori-teori pendukung lainnya.

### 2.2 *Advanced Encryption Standard* (AES)

Algoritme *Advanced Encryption Standard* (AES) adalah suatu algoritme *block cipher* dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Penyediaan AES menggunakan proses yang berulang yang disebut dengan *ronde*. Jumlah *ronde* yang digunakan oleh AES tergantung dengan panjang kunci yang digunakan. Setiap *ronde* membutuhkan kunci dan memasukan dari *ronde* berikutnya. Kunci *ronde* dibangkitkan berdasarkan kunci yang diberikan. Algoritme AES dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Panjang kunci mempengaruhi jumlah *round* (perputaran), perbedaan dari ketiga kunci tersebut dapat digambarkan dalam Tabel 1 Perbandingan jumlah kunci AES[4].

Tabel 1. Perbandingan Pada Jumlah Kunci AES

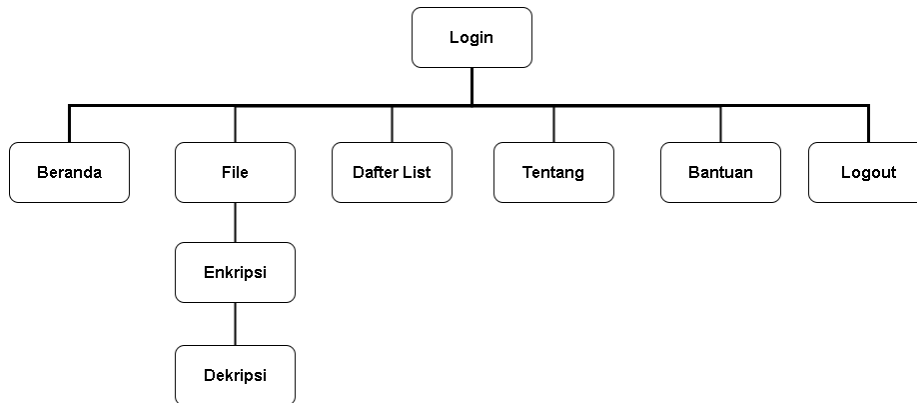
AES(bits)	Panjang Kunci (Nk Words)	Ukuran Blok (Nb Words)	Jumlah Putaran (NR)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

*Advance Encryption Standard* (AES) merupakan kelanjutan dari algoritme enkripsi *Data Encrytion Standard* (DES), yang dianggap sudah lawas karena faktor keamanannya. Kecepatan dari sebuah komputer yang sangat tinggi dianggap terlalu berbahaya untuk DES, sehingga pada saat tanggal 2 Maret 2001, algoritme Rijndael yang

baru diterapkan yaitu AES. Kriteria seleksi untuk AES didasarkan pada tiga kriteria utama, keamanan, biaya, dan karakteristik algoritme dan penerapannya[2].

### 2.3 Rancangan Menu

Pada rancangan menu aplikasi yang akan dibuat terdiri dari beberapa tampilan menu yang dapat dilihat pada bagian gambar 2.



Gambar 2. Rancangan Menu

### 2.4 Rancangan Basis Data

Berikut ini adalah struktur-struktur tabel yang terdapat di dalam basis data yang akan digunakan pada aplikasi ini. Nama basis data yang di gunakan yaitu aes, lalu untuk tabel user bisa dilihat pada tabel 2

Tabel 2. Spesifikasi Basis Data Tabel users

Nama Field	Tipe	Keterangan
username	Varchar(15)	Username
password	Varchar(100)	Password
fullname	Varchar(50)	Nama User
job_title	Varchar(50)	Nama Jabatan
job_activity	Timestamp	Tanggal Gabung
last_activity	Timestamp	Activitas terakhir
status	Enum(1,2)	Admin

Pada tabel 3 akan di gunakan untuk mangidentifikasi file yang akan di enkripsi, dan menghindari terjadi data ganda yang tersimpan.

Tabel 3. Spesifikasi Basis Data Tabel file

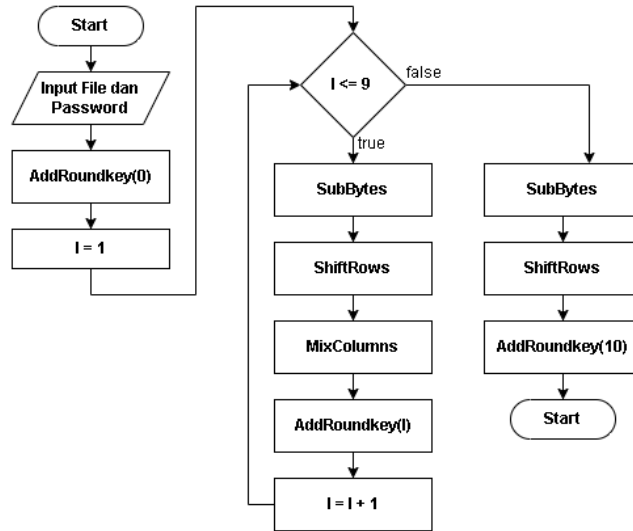
Nama Field	Tipe	Keterangan
id_file	Int(11)	Id File
username	Varchar(15)	Username
file_name_source	Varchar(255)	Nama file Asli
file_name_finish	Varchar(255)	Nama Hasil file
file_url	Varchar(255)	url File
file_size	Float	Ukuran
password	Varchar(16)	Password
tgl_upload	Timestamp	Tanggal Upload
status	Enum(1,2)	Enkripsi dan Dekripsi
keterangan	Varchar(255)	Keterangan

## 3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi analisis, hasil implementasi ataupun pengujian serta pembahasan dari topik penelitian, yang bisa dibuat terlebih dahulu metodologi penelitian. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

### 3.1 Flowchart Enkripsi AES-128

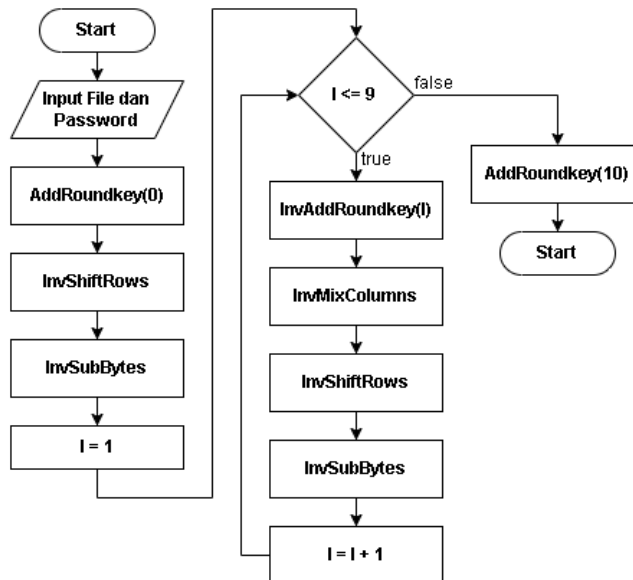
Pada alur proses enkripsi AES-128 ini terdapat pada gambar 3. Flowchart ini menjelaskan tentang enkripsi AES-128 pada aplikasi ini.



Gambar 3. Flowchart Enkripsi AES-128

### 3.2 Flowchart Dekripsi AES-128

Pada alur proses dekripsi AES-128 ini terdapat pada Gambar 4. Flowchart ini menjelaskan tentang dekripsi AES-128 pada aplikasi ini.



Gambar 4. Flowchart Dekripsi AES-128

### 3.3 Algoritme Enkripsi AES-128

Pada algoritme bagian ini akan menjelaskan tentang bagaimana alur dari proses yang terjadi pada enkripsi aes-128.

Algoritme 1. Enkripsi AES-128

1	Start
2	Input File dan Password
3	AddRoundkey(0)
4	I=1
5	If I <= 9
6	SubBytes
7	ShiftRows
8	MixColumns
9	AddRoundKey(I)
10	I = I + 1
11	Kembali ke baris 5
12	Else
13	SubBytes
14	ShiftRows
15	AddRoundKey(10)
16	End

### 3.4 Algoritme Dekripsi AES-128

Pada algoritme bagian ini akan menjelaskan tentang bagaimana alur dari proses yang terjadi pada dekripsi aes-128.

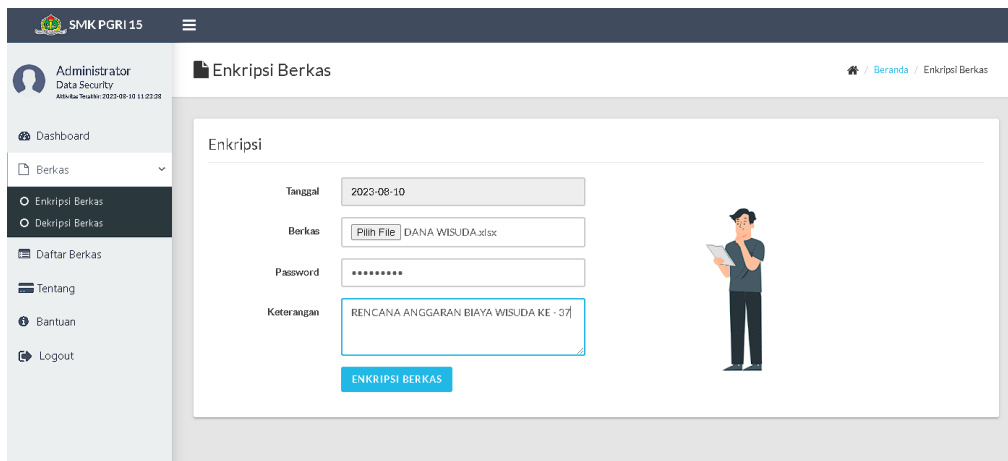
**Algoritme 2.** Dekripsi AES-128

1	Start
2	Input File dan Password
3	AddRoundkey(0)
4	InvShiftRows
5	InvSubBytes
6	I=1
7	If I<=9
8	AddRoundKey(I)
9	InvMixColumns
10	InvShiftRows
11	InvSubBytes
12	I=I+1
13	Kembali ke baris 7
14	Else
15	AddRoundKey(10)
16	End

### 3.5 Implementasi Metode

#### 3.5.1 Proses Enkripsi

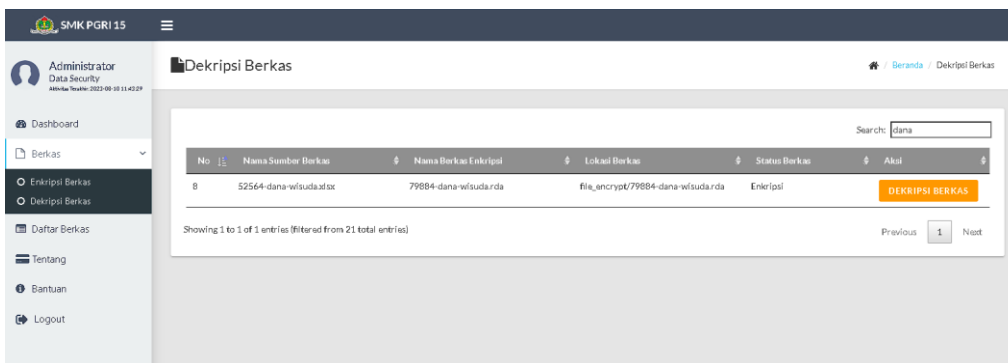
Pada saat melakukan enkripsi *user* harus login terlebih dahulu. Kemudian masuk menu enkripsi yang terletak pada bagian sub menu berkas. Akan tampil form enkripsi untuk mengisi *file*, *password*, keterangan dan untuk tanggal akan terisi otomatis.



Gambar 5. Halaman form enkripsi

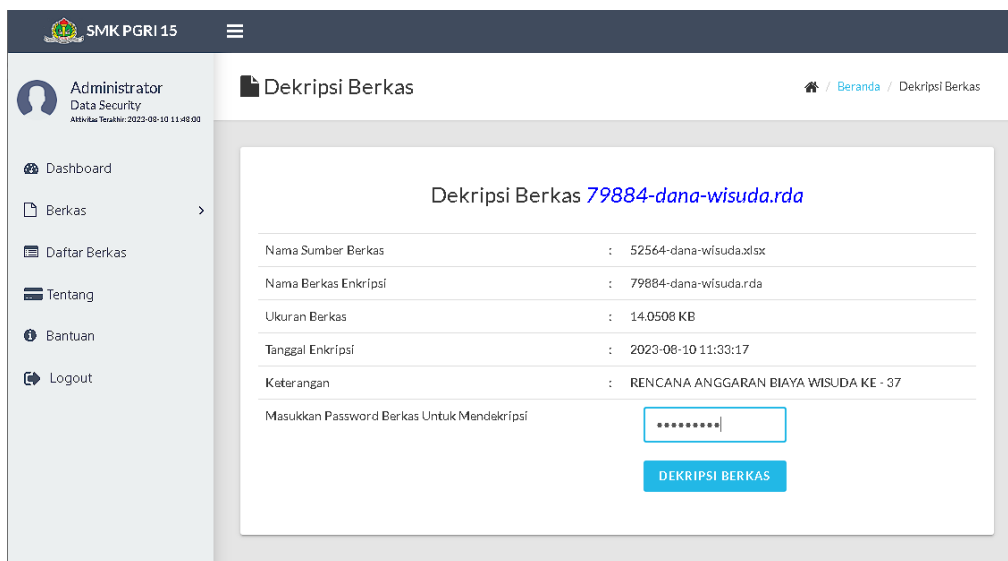
### 3.5.2 Proses Dekripsi

Untuk proses dekripsi, user perlu memilih file yang akan di dekripsi yang berada di menu berkas, yang terletak pada sub menu berkas. Kemudian klik tombol 'DEKRIPSI BERKAS' maka akan masuk ke halaman informasi tentang berkas yang akan di dekripsi.



Gambar 6. Halaman tabel dekripsi

Berikut ini merupakan informasi dari file yang akan di dekripsi. Untuk melakukan dekripsi diperlukan password yang sama saat melakukan enkripsi.



Gambar 7. Halaman informasi berkas

### 3.6 Pengujian Program

Setelah kebutuhan terpenuhi baik software maupun hardware, maka proses selanjutnya adalah mengujian coba aplikasi yang telah dibuat. Pada bagian ini dapat diuraikan mengenai pengujian aplikasi enkripsi dekripsi. Pengujian tersebut nantinya akan mendapatkan hasil enkripsi dari file yang akan dienkripsi. Dan kecepatan berapa lama file tersebut dienkripsi maupun juga pada saat di dekripsi.

#### 3.6.1 Tabel Pengujian Enkripsi

Pada tabel 4 merupakan hasil dari proses pengujian enkripsi yang dikerjakan oleh sistem.

**Tabel 4.** Hasil Enkripsi

No	Nama File Asli	Ukuran Asli (KB)	Waktu (detik)	Nama File Enkripsi	Ukuran File Enkripsi (KB)	Kecepatan (KB/detik)
1	DANA WISUDA.xlsx	14	2,32	79884-dana-wisuda.rda	14	6,03
2	DENAH SMK PGRI 15 JAKARTA.jpg	4.012	100,91	29571-denah-smk-pgri-15-jakarta.rda	4.012	39,76
3	FORMULIR LAPOR DIRI.pdf	382	8,51	13722-formulir-lapor-diri.rda	383	44,89
4	laporan spp siswa kelas x.xlsx	16,7	1,44	41841-laporan-spp-siswa-kelas-x.rda	16,7	11,60
5	LOGO SMK PGRI 15 JAKARTA.png	77,3	2,83	28288-logo-smk-pgri-15-jakarta.rda	77,3	27,31
6	Nilai XI AKUNTANSI DAN KEUANGAN LEMBAGA AKL - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	34	1,44	74833-nilai-xi-akuntansi-dan-keuangan-lembaga-akl---pendidikan-agama-dan-budi-pekerti.rda	34	23,61
7	Nilai XI BISNIS DARING DAN PEMASARAN BDP 1 - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	30	1,21	26685-nilai-xi-bisnis-daring-dan-pemasaran-bdp-1---pendidikan-agama-dan-budi-pekerti.rda	30	24,79
8	Nilai XI BISNIS DARING DAN PEMASARAN BDP 2 - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	29,5	1,56	12593-nilai-xi-bisnis-daring-dan-pemasaran-bdp-2---pendidikan-agama-dan-budi-pekerti.rda	29,5	18,91
9	Nilai XI OTOMATISASI DAN TATA KELOLA PERKANTORAN OTKP 1 - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	31,5	1,93	20659-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-1---pendidikan-agama-dan-budi-pekerti.rda	31,5	16,32
10	Nilai XI OTOMATISASI DAN TATA KELOLA PERKANTORAN OTKP 2 - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	31,5	1,82	30094-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-2---pendidikan-agama-dan-budi-pekerti.rda	31,5	17,31
11	Nilai XI OTOMATISASI DAN TATA KELOLA PERKANTORAN OTKP 3 -	32	1,18	49090-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-3---pendidikan-	32	27,12

	PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls			agama-dan-budi- pekerti.rda		
12	Nilai XI PERHOTELAN PH 1 - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	31,5	1,02	69416-nilai-xi- perhotelan-ph-1--- pendidikan-agama- dan-budi-pekerti.rda	31,5	30,88
13	Nilai XI PERHOTELAN PH 2 - PENDIDIKAN AGAMA DAN BUDI PEKERTI.xls	31	1,11	57247-nilai-xi- perhotelan-ph-2--- pendidikan-agama- dan-budi-pekerti.rda	31	27,93
14	PRESENTASI KESISWAAN.pptx	1.030	24,56	33746-presentasi- kesiswaan.rda	1.030	41,94
15	SOAL EKONOMI DAN PEMBARUAN ISLAM.docx	19,5	1,17	64609-soal-ekonomi- dan-pembaruan- islam.rda	19,5	16,67
16	SOAL MASA KEJAYAAN ISLAM.docx	17,1	0,84	45312-soal-masa- kejayaan-islam.rda	17,1	20,36
17	Soal Materi Bekerja Keras dan Tanggung Jawab.docx	19,9	1,01	6906-soal-materi- bekerja-keras-dan- tanggung-jawab.rda	19,9	19,70
18	SOAL PAI KELAS 12 SMK PGRI 15 JAKARTA.docx	93,6	2,53	20639-soal-pai-kelas- 12-smk-pgri-15- jakarta.rda	93,6	37,00
19	SURAT CUTI.docx	14,3	2,06	52380-surat-cuti.rda	14,3	6,94
20	TEMA WISUDA SMK PGRI 15 JAKARTA 2023.doc	26,5	1,41	93875-tema-wisuda- smk-pgri-15-jakarta- 2023.rda	26,5	18,79

### 3.6.2 Tabel Pengujian Dekripsi

Pada tabel 5 merupakan hasil dari proses pengujian dekripsi yang dikerjakan oleh sistem.

**Tabel 5.** Hasil Dekripsi

No	Nama File Dekripsi	Ukuran Awal (KB)	Waktu (detik)	Nama File Asli	Ukuran Akhir (KB)	Kecepatan (KB/detik)
1	79884-dana-wisuda.rda	14	2,37	52564-dana- wisuda.xlsx	14	5,91
2	29571-denah-smk-pgri- 15-jakarta.rda	4.012	100,94	79655-denah-smk- pgri-15-jakarta.jpg	4.012	39,75
3	13722-formulir-lapor- diri.rda	382	8,47	54150-formulir-lapor- diri.pdf	382	45,10
4	41841-laporan-spp- siswa-kelas-x.rda	16,7	1,33	47076-laporan-spp- siswa-kelas-x.xlsx	16,7	12,56
5	28288-logo-smk-pgri- 15-jakarta.rda	77,3	2,94	37317-logo-smk-pgri- 15-jakarta.png	77,3	26,29
6	74833-nilai-xi- akuntansi-dan- keuangan-lembaga-akl- -pendidikan-agama- dan-budi-pekerti.rda	34	1,52	30013-nilai-xi- akuntansi-dan- keuangan-lembaga- akl---pendidikan- agama-dan-budi- pekerti.xls	34	22,37
7	26685-nilai-xi-bisnis- daring-dan-pemasaran- bdp-1---pendidikan- agama-dan-budi- pekerti.rda	30	1,28	45929-nilai-xi-bisnis- daring-dan- pemasaran-bdp-1--- pendidikan-agama- dan-budi-pekerti.xls	30	23,44
8	12593-nilai-xi-bisnis- daring-dan-pemasaran- bdp-2---pendidikan-	29,5	1,51	57102-nilai-xi-bisnis- daring-dan- pemasaran-bdp-2---	29,5	19,54



9	agama-dan-budi-pekerti.rda 20659-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-1---pendidikan-agama-dan-budi-pekerti.rda	31,5	1,82	pendidikan-agama-dan-budi-pekerti.xls 73321-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-1---pendidikan-agama-dan-budi-pekerti.xls	31,5	17,31
10	30094-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-2---pendidikan-agama-dan-budi-pekerti.rda	31,5	1,91	49758-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-2---pendidikan-agama-dan-budi-pekerti.xls	31,5	16,49
11	49090-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-3---pendidikan-agama-dan-budi-pekerti.rda	32	1,14	40803-nilai-xi-otomatisasi-dan-tata-kelola-perkantoran-otkp-3---pendidikan-agama-dan-budi-pekerti.xls	32	28,07
12	69416-nilai-xi-perhotelan-ph-1---pendidikan-agama-dan-budi-pekerti.rda	31,5	1,09	81347-nilai-xi-perhotelan-ph-1---pendidikan-agama-dan-budi-pekerti.xls	31,5	28,90
13	57247-nilai-xi-perhotelan-ph-2---pendidikan-agama-dan-budi-pekerti.rda	31	1,21	31697-nilai-xi-perhotelan-ph-2---pendidikan-agama-dan-budi-pekerti.xls	31	25,62
14	33746-presentasi-kesiswaan.rda	1.030	24,62	6211-presentasi-kesiswaan.pptx	1.030	41,84
15	64609-soal-ekonomi-dan-pembaruan-islam.rda	19,5	1,23	95394-soal-ekonomi-dan-pembaruan-islam.docx	19,5	15,85
16	45312-soal-masa-kejayaan-islam.rda	17,1	0,98	67050-soal-masa-kejayaan-islam.docx	17,1	17,45
17	6906-soal-materi-bekerja-keras-dan-tanggung-jawab.rda	19,9	1,09	56677-soal-materi-bekerja-keras-dan-tanggung-jawab.docx	19,9	18,26
18	20639-soal-pai-kelas-12-smk-pgri-15-jakarta.rda	93,6	2,48	53817-soal-pai-kelas-12-smk-pgri-15-jakarta.docx	93,6	37,74
19	52380-surat-cuti.rda	14,3	2,13	52172-surat-cuti.docx	14,3	6,71
20	93875-tema-wisuda-smk-pgri-15-jakarta-2023.rda	26,5	1,49	91181-tema-wisuda-smk-pgri-15-jakarta-2023.doc	26,5	17,79

#### 4. KESIMPULAN

Berdasarkan penjelasan dan uraian dari penelitian ini, maka dapat disimpulkan bahwa dengan adanya aplikasi kriptografi proses penyimpanan dan pertukaran informasi menjadi lebih aman. Waktu yang diperoleh untuk melakukan proses enkripsi dan dekripsi berbanding lurus dengan ukuran file yang diproses (semakin kecil ukuran file yang diproses, makin kecil proses enkripsi dan dekripsinya, semakin besar ukuran file, makin lama proses enkripsi dan dekripsinya). Format file yang dapat digunakan pada aplikasi ini berupa file dokumen *office* dengan ekstensi \*.doc, \*.xls, \*.ppt, \*.docx, \*.xlsx, \*.pptx, \*.pdf dan juga file gambar seperti \*.png, \*.jpg. Diharapkan aplikasi ini dapat berkembang tidak hanya bisa digunakan pada dokumen tulisan, namun bisa digunakan pada dokumen berbentuk video atau audio.

## DAFTAR PUSTAKA

- [1] Yuningrat Dwi Putri, Rosihan, Salkin Lutfi, "PENERAPAN KRIPTOGRAFI CAESAR CIPHER PADA FITUR CHATTING SISTEM INFORMASI FREELANCE", *Jurnal Informatika dan Komputer*, Vol. 2, 87-94, 2019
- [2] Wijaya, P. A., Damanik, M., Hartati, P., & Gunawan, I., "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection", *Akademika Jurnal*, Vol. 17, 8-13, 2020
- [3] Delisman Hulu, Berto Nadeak, Soeb Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSUD Imelda Medan", *KOMIK*, Vol. 4, 78-86, 2020
- [4] B. E. Widodo and A. S. Purnomo, (2020). "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy", *Jurnal Teknik Informatika*, Vol. 1, 70-72, 2020
- [5] Dedy Ronald Saragi, Janter Mamiel Gultom, Jose Andreas Tampubolon, Indra Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritme RC4", *Jurnal Sistem Komputer dan Informatika*, Vol. 1, 114-119, 2020
- [6] Eko Hartatoa, Indra Gunawanb, Iin Parlinac, Solikhund, Anjar Wantoe. (2020) "Analisis Algoritma AES Dalam Mengamankan Data Pada Kantor Walikota Pematangsiantar", *JURNAL ILMIAH INFORMATIKA*, Vol. 08, 19-21, 2020
- [7] Muhammad Azhari, Dadang Iskandar Mulyana, Faizal Joko Perwitosari, Firhan Ali, "Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritme Kriptografi Advanced Encryption Standard(AES)", *Jurnal Pendidikan Sains dan Komputer*, Vol. 2, 163-171, 2022
- [8] Aditia Rahmat Tulloh, Yurika Permanasari, Erwin Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen", *Jurnal Matematika UNISBA*, Vol. 15, 8-14, 2016
- [9] Andi Inayah Auliyah, "Implementasi Kombinasi Algoritme Enkripsi Rivest Shamir Adleman (RSA) dan Algoritme Kompresi Huffman Pada File Document", *Indonesian Journal of Data and Science*, Vol.1, 23-28, 2020
- [10] Azanuddin, Suardi Yakud dan Jaka Prayudha, "Implementasi Keamanan Citra Menggunakan Algoritme AES-128 Dengan Aplikasi Client-Server", *Jurnal Riset Sistem Informasi Dan Teknik Informatika*, Vol. 7, pp 51-61, 2022