Hello World
Jurnal Ilmu Komputer
https://jurnal.ilmubersama.com/index.php/hello_world

Keamanan Komputer

Implementasi Kombinasi Algoritma Rinjdael dengan Caesar Cipher pada Pengamanan Dokumen Digital

Rido Maruli Tua Pasaribu [1], Rafiqa Dewi [2], Iin Parlina [3]

[1] *Program Studi Teknik Informatika, STIKOM Tunas Bangsa, Pematangsiantar, Indonesia*
[2] *Program Studi Manajemen Informatika, AMIK Tunas Bangsa, Pematangsiantar, Indonesia*
[3] *Program Studi Komputerisasi Akuntansi, AMIK Tunas Bangsa, Pematangsiantar, Indonesia*

INFORMASI ARTIKEL

Diterima Redaksi: 15 Mei 2022
Revisi Akhir: 18 Mei 2022
Diterbitkan *Online*: 20 Mei 2022

KATA KUNCI

Rijndael; AES-128 bit; Caesar Cipher; Kriptografi

KORESPONDENSI

Phone: +62 852-6260-2867
E-mail: micaryus20@gmail.com

A B S T R A K

Keamanan file dokumen digital merupakan hal yang sangat penting sejalan dengan perkembangan teknologi informasi saat ini. Ada banyak metode dalam mengamankan data digital, salah satunya adalah Kriptografi. Algoritma Rinjdael atau Advanced Encryption Standart adalah metode yang dapat digunakan untuk mengamankan file dokumen digital. Algoritma Rinjdael ditetapkan sebagai AES sebagai pengganti Algoritma DES dengan lebih banyak kunci, yakni kunci 128-bit, 192-bit dan 256-bit. Penelitian ini dilakukan untuk mengamankan file dokumen dengan menggunakan kombinasi dua algoritma, yaitu Algoritma Rinjdael dan Caesar Cipher. Kombinasi kedua algoritma tersebut akan mengembangkan proses enkripsi file menjadi lebih kompleks sehingga file dokumen digital menjadi lebih terjamin keamanannya. Proses enkripsi yang lebih kompleks dapat meminimalisir potensi serangan eksternal seperti ancaman Brute Force, dan lain-lain.

PENDAHULUAN

Berdasarkan era masyarakat berbasis informasi saat ini, sebuah dokumen digital merupakan komponen yang sangat vital, sehingga memerlukan sistem keamanan yang baik saat didistribusikan ataupun saat disimpan [1]. Akhirnya dikembangkan berbagai metode untuk mengatasi persoalan keamanan data yang pada intinya adalah cara untuk mengantisipasi agar pihak-pihak yang tidak berhak, tidak dapat membaca atau bahkan merusak data yang bukan ditujukan kepadanya. Salah satu cara pengamanan data tersebut adalah dengan menerapkan kriptografi/penyandian.

Sejalan dengan perkembangan ilmu pengetahuan dan teknologi saat ini, tindak kriminalitas di dunia maya juga semakin banyak dengan motif yang juga beragam. Salah satu cybercrime yang marak terjadi saat ini adalah pencurian data digital, seperti dokumen perusahaan, data informasi perusahaan dan sebagainya [2]. Seperti pada SMK Negeri 3 Pematangsiantar karena keterbatasan pengamanan dokumen digital, terdapat orang yang tidak berkepentingan yang mengambil sebuah dokumen digital tanpa seijin pegawai. Hal seperti ini sering dilakukan oleh sekelompok atau pihak-pihak yang tidak bertanggungjawab demi meraup keuntungan pribadi.

Ada Banyak cabang dibidang ilmu komputer yang mampu menyelesaikan masalah yang kompleks, hal ini terbukti dari banyaknya penelitian-penelitian yang sudah pernah dilakukan, seperti bidang sistem pendukung keputusan [3]–[10], bidang jaringan saraf tiruan [11]–[20], bidang data mining [24]–[31], bidang keamanan komputer [32]–[35], dan masih banyak lagi yang lain nya.

Keamanan informasi merupakan suatu perlindungan informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah untuk memberikan kerahasiaan, integritas, dan ketersediaan informasi

https://doi.org/10.56211/helloworld.v1i1.11

[32]. Keamanan informasi merupakan satu hal yang sangat penting yang harus dilakukan. Pada era sekarang ini sangat rawan pencurian dan penyalahgunaan data dari orang-orang yang tidak bertanggung jawab [33]. Akan tetapi, kasus keamanan ini kurang menerima perhatian menurut para pemilik dan pengelola sistem informasi, serta banyaknya perusahaan yang menghubungkan sistem informasinya dengan jaringan internet. Hal ini membuka akses secara global (maksud akses ini menjadi target dan pula menjadi penyerang). Untuk mencegah terjadinya pencurian dan penyalahgunaan data digital, maka digunakan algoritma Kriptografi untuk proses enkripsi dan proses dekripsi data [34]. Algoritma Kriptografi bertujuan supaya hanya orang yang berkepentingan terhadap data digital tersebut yang dapat mengaksesnya dengan kunci enkripsi yang sudah ditentukan [35].

Beberapa penelitian terdahulu yang menjadi rujukan dilakukannya penelitian ini, antara lain: Penelitian dengan menggunakan algoritma kriptografi rijndael dan twofish untuk penyandian data [36]. Selanjutnya penelitian yang dilakukan dengan menerapkan algoritma caesar cipher dan steganografi least significant bit untuk file dokumen [37]. Penelitian berikutnya dilakukan untuk menganalisis dan mengimplementasikan Algoritma Rijndael (AES) dan Kriptografi RSA untuk Pengamanan File [38].

Berdasarkan uraian latar belakang tersebut, maka dilakukan penelitian untuk mengamankan dokumen digital menggunakan Kombinasi Algoritma Rinjdael Dengan Caesar Cipher. Penelitian ini diharapkan dapat membantu pihak terkait dalam melakukan pengamanan data digital.

METODOLOGI

Lokasi dan Waktu Penelitian

Penelitian ini dilakukan di SMK Negeri 3 Pematangsiantar, dengan waktu penelitian pada tanggal 01 Maret 2021 – 06 Maret 2021 (6 Hari).

Prosedur Pengumpulan Data

1. Wawancara
   Adapun konteks untuk melakukan wawancara dengan narasumber sebagai berikut, dapat dilihat pada tabel 1 berikut.

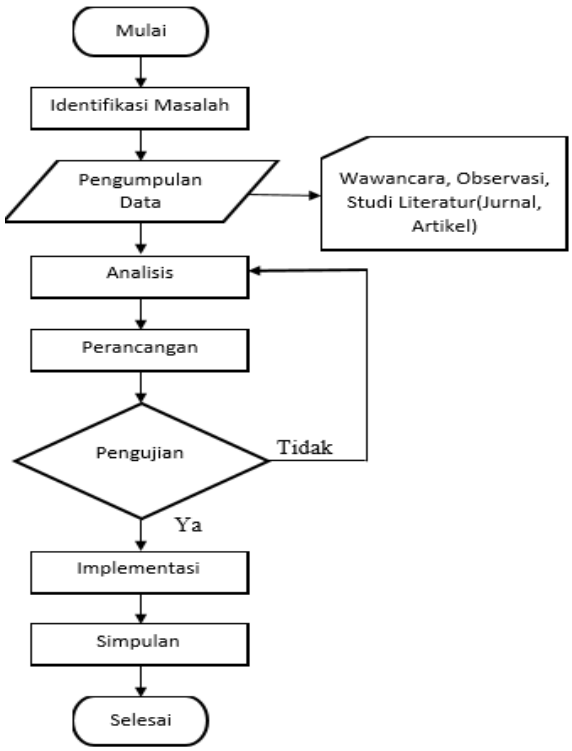
Tabel 1. Konteks Wawancara

No	Informan	Konteks Wawancara
1	Bagian Administrasi Keuangan	Terkait dengan data – data dan dokumen digital keuangan yang bersifat rahasia.
2	Bagian Administrasi Kepegawaian	Terkait dengan data – data dan dokumen digital kepegawaian yang bersifat rahasia

2. Observasi
   Adapun pelaksanaan observasi yang dilakukan terfokus pada data – data dan dokumen digital pada bagian Tata Usaha SMK Negeri 3 Pematangsiantar. Adapun data – data dan dokumen digital yang akan digunakan dalam penelitian ini adalah sebagai berikut.
   a. Data Kepegawaian
      Setelah penulis melakukan wawancara dengan Tata Usaha bagian administrasi di SMK Negeri 3 Pematangsiantar dan berdasarkan hasil observasi, terdapat beberapa data dan dokumen digital yang bersifat rahasia. Adapun diantaranya Surat Penugasan Tenaga Pendidik, Data Akun Pendidik, dan sebagainya.
   b. Data Keuangan
      Setelah dilakukan wawancara dengan administrasi kepegawaian di bagian Tata Usaha SMK Negeri 3 Pematangsiantar dan hasil observasi penulis, terdapat beberapa data dan dokumen digital yang bersifat rahasia. Adapun diantaranya Data Perincian Gaji Guru dan Pegawai, dan sebagainya.

Rancangan Penelitian

Rancangan penelitian yang dilakukan untuk menyelesaikan permasalahan pada penelitian ini adalah sebagai berikut.



Gambar 1. Kerangka Penelitian

Penjelasan :

1. Identifikasi Masalah
   Maraknya pencurian data dan penyalahgunaan dokumen digital menyebabkan kerugian si pemilik dokumen. Pada tahapan awal penulis melakukan pengamatan secara langsung terhadap instansi yang bersangkutan terfokus paa masalah keamanan dokumen digital.
2. Pengumpulan Data
   Pada tahap ini data yang akan diamankan diambil dari SMK Negeri 3 Pematangsiantar dengan menggunakan metode pengumpulan data melalui wawancara, dan observasi yang diperlukan dalam membantu memecahkan permasalahan.
3. Analisis
   Pada tahapan ini terlebih dahulu dilakukan analisis terhadap algoritma Advanced Encryption Standard (AES) dan Caesar Cipher sehingga dapat diimplementasikan pada keamanan dokumen digital.
4. Perancangan
   Pada tahap ini akan dijelaskan apa yang akan dirancang oleh penulis dengan menggunakan aplikasi Microsoft Visual Studio dengan bahasa pemrograman VB.Net.
5. Pengujian
   Pada tahap ini dilakukan pengujian aplikasi keamanan dokumen digital
6. Implementasi
   Pada tahapan ini penulis melewati beberapa tahapan implementasi di antaranya adalah persiapan menginstal Microsoft Visual Studio 2015 dan perancangan program dengan membangun aplikasi sesuai pada fitur yang ditentukan.
7. Simpulan
   Pada tahap ini dilakukan penarikan kesimpulan akhir yang diperoleh setelah melakukan tahap analisis, perancangan, pengujian dan implementasi aplikasi yang dirancang dengan menerapkan algoritma AES dan Caesar Cipher.

Algoritma Sistem

Untuk menerapkan sistem keamanan ke dalam program aplikasi maka dibutuhkan suatu kombinasi algoritma, yaitu kombinasi langkah-langkah atau instruksi yang akan digunakan untuk mengenkripsi dan mendeskripsikan data-data dan dokumen digital yang bersifat rahasia. Algoritma yang digunakan dalam penelitian ini adalah algoritma kriptografi Advanced Encryption Standard (AES) 128-bit dan Caesar Cipher.

HASIL DAN PEMBAHASAN

Pengolahan Data

Perhitungan dalam algoritma Rinjdael (AES 128-Bit) dan Caesar Cipher diuraikan dengan cukup detail dimulai dari perhitungan algoritma Caesar Cipher yang berfungsi mengenkripsi Key, dan perhitungan algoritma Rinjdael (AES 128-Bit) yang berfungsi mengenkripsi Dokumen Digital.

Untuk menerapkan sistem keamanan ke dalam program aplikasi maka dibutuhkan suatu kombinasi algoritma, yaitu kombinasi langkah-langkah atau instruksi yang akan digunakan untuk mengenkripsi dan mendekripsikan data-data dan dokumen digital yang bersifat rahasia. Algoritma yang digunakan dalam penelitian ini adalah algoritma kriptografi Advanced Encryption Standard (AES) 128-bit dan Caesar Cipher.

Contoh perhitungan enkripsi dengan kombinasi algoritma Rinjdael (AES 128-Bit) dan Caesar Cipher dapat dilihat pada proses berikut.

1. Konversi dengan Caesar Cipher
   Sebagai contoh plainteks (dokumen digital) dan kunci yang digunakan pada contoh ini adalah seperti berikut:
   Plainteks : SEKOLAH MENENGAH
   Kunci : PEMATANG SIANTAR
   Langkah awal yang dilakukan adalah dengan mengubah kunci dengan algoritma Caesar Cipher dengan pergeseran 5 root word sehingga menjadi seperti berikut.
   Kunci : UJRFYFSL%XNFSYFW
2. Konversi dengan Heksadesimal
   Langkah selanjutnya mengubah plainteks (dokumen digital) dan kunci tersebut menjadi bentuk heksadesimal. Konversi plainteks ke dalam bentuk heksadesimal dapat disesuaikan pada tabel ASCII, dapat dilihat pada tabel berikut.

Tabel 2. Tabel ASCII

Dec	Hex	Character
32	20	Spasi
33	21	!
34	22	“
35	23	#
36	24	$
37	25	%
38	26	`
39	27	(
40	28	)
41	29	*
42	2A	+
43	2B	‘
44	2C	-
45	2D	.
46	2E	/
47	2F	
48	30	0
49	31	1
50	32	2
51	33	3
52	34	4
53	35	5
54	36	6
55	37	7
56	38	8
57	39	9
58	3A	:
59	3B	;
60	3C	<
61	3D	=
62	3E	>
63	3F	?
64	40	@
65	41	A
66	42	B

Dec	Hex	Character
67	43	C
68	44	D
69	45	E
70	46	F
71	47	G
72	48	H
73	49	I
74	4A	J
75	4B	K
76	4C	L
77	4D	M
78	4E	N
79	4F	O
80	50	P
81	51	Q
82	52	R
83	53	S
84	54	T
85	55	U
86	56	V
87	57	W
88	58	X
89	59	Y
90	5A	Z
91	5B	[
92	5C	\
93	5D	]
94	5E	^
95	5F	_
96	60	`
97	61	a
98	62	b
99	63	c
100	64	d
101	65	e
102	66	f
103	67	g
104	68	h
105	69	i
106	6A	j
107	6B	k
108	6C	l
109	6D	m
110	6E	n
111	6F	o
112	70	p
113	71	q
114	72	r
115	73	s
116	74	t
117	75	u
118	76	v
119	77	w
120	78	x
121	79	y
122	7A	z

Hasil konversi plainteks dan kunci di atas adalah sebagai berikut :

Plainteks : 53 45 4B 4F 4C 41 48 20 4D 45 4E 45 4E 47 41 48

Kunci : 55 4A 52 46 59 46 53 4C 25 58 4E 46 53 59 46 57

Setelah mengkonversi plainteks dan kunci ke dalam bentuk heksadesimal, maka selanjutnya plainteks dan kunci diubah ke dalam bentuk matriks berordo 4x4 seperti di bawah ini.

55	59	25	53
4A	46	58	59
52	53	4E	46
46	4C	46	57

Plainteks

53	4C	4D	4E
45	41	45	47
48	48	4E	41
4F	20	45	48

Kunci

 https://doi.org/10.56211/helloworld.v1i1.11

3. Tahapan enkripsi algoritma *Rinjdael* (*AES 128-Bit)* terbagi dalam empat jenis proses, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*. Sebelum melakukan enkripsi perlu dilakukan ekspansi atau pembangkitan kunci, hal ini bertujuan untuk mendapatkan kunci ronde atau *round key* yang akan digunakan pada tahap transformasi *AddRoundKey*.
4. Ekspansi Kunci
   Algoritma *Rinjdael (AES-128 Bit)* menggunakan *cipher key* dan membuat suatu ekspansi kunci untuk menghasilkan suatu *key schedule.* Ekspansi kunci yang diperlukan *AES-128 Bit* adalah 1*408 bit subkey*. Proses ekspansi dari 128 *bit* menjadi 1408 *bit subkey* ini disebut dengan *key schedule.*

55	59	25	53
4a	46	58	59
52	53	4e	46
46	4c	46	57
Cipher Key			

9F	C6	E3	B0
10	56	0E	57
09	5A	14	52
AB	E7	A1	F6
RoundKey1			

C6	00	E3	53
10	46	48	1F
4B	11	05	57
4C	AB	0A	FC
RoundKey2			

02	02	E1	B2
4B	0D	45	5A
FB	EA	EF	B8
A1	0A	00	FC
RoundKey3			

B4	B6	57	E5
27	2A	6F	35
4B	A1	4E	F6
96	9C	9C	60
RoundKey4			

32	84	D3	36
65	4F	20	15
9B	3A	74	82
4F	D3	4F	2F
RoundKey5			

4B	CF	1C	2A
76	39	19	0C
8E	B4	C0	42
4A	99	D6	F9
RoundKey6			

F5	3A	26	0C
5A	63	7A	76
17	A3	63	21
AF	36	E0	19
RoundKey7			

4D	77	51	5D
A7	C4	BE	C8
C3	60	03	22
51	67	87	9E
RoundKey8			

BE	C9	98	C5
34	F0	4E	86
C8	A8	AB	89
1D	7A	FD	63
RoundKey9			

Gambar 2. Ekspansi Kunci *AES 128-Bit*

Proses ekspansi kunci algoritma *Rinjdael (AES 128-Bit)* terdiri dari:

a. *RotWord( )* mengambil *input* 4 *byte word* [0a,a1,a2,a3] dan membentuk *cyclic* permutasi menjadi [a1,a2,a3,a0]
b. *SubWord( )* mengambil *input* 4 *byte word* dan melakukan operasi substitusi menggunakan tabel *S-Box* sehingga didapat 4 *byte output* dari prosedur
c. *Rcon( )* menghasilkan *round* yang tetap dari *word array* dan berisi nilai yang diberikan oleh [(wi-1) XOR (01, 00, 00, 00) XOR (wi-4)].

01	02	04	08	10	20	40	80	1b	36
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

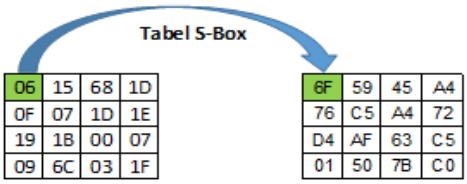
Gambar 3. *Round Constant (Rcon)*

5. Transformasi *SubBytes*
   Pada tahapan ini, seluruh *key* sudah dibangkitkan sebanyak 10 *round key*. Selanjutnya dilakukan proses enkripsi dimulai dari proses *SubBytes*. Transformasi *SubBytes* memetakan setiap *byte* dari *array state* dengan menggunakan tabel substitusi *S-Box Rijndael* yang dapat dilihat pada gambar 4 berikut.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 4. *S-Box Rijndael*

Tahapan pensubstitusian adalah sebagai berikut : Jika setiap *byte* pada *array state* S[rows, columns] = xy, dengan xy adalah digit heksadesimal dari nilai S[r,c] maka nilai substitusinya dinyatakan dengan S'[r,c] yaitu elemen di dalam *S-Box* yang merupakan perpotongan baris x dengan kolom y seperti yang dapat dilihat pada gambar 5 berikut.



Gambar 5. Transformasi *SubBytes* dengan *S-Box*

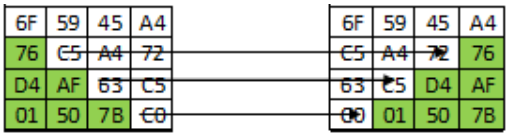
Setiap S[(r)baris,(c)kolom] dilakukan operasi substitusi dengan tabel *S-Box* sehingga menghasilkan S[0,6]=S[6,f], dst. Hasil dari transformasi *SubBytes* dapat dilihat pada gambar 6 berikut.

6F	59	45	A4
76	C5	A4	72
D4	AF	63	C5
01	50	7B	C0

Gambar 6. Hasil *SubBytes* dengan tabel *S-Box*

6. Transformasi *ShiftRows*

Transformasi *ShiftRows* adalah tahapan yang melakukan pergeseran secara *wrapping* pada 3 (ketiga) baris terakhir dari *array state.* Jumlah pergeseran bergantung pada nilai baris r. Baris r=1 digeser sejarak 1 *byte*, baris r=2 digeser sejarak 2 *byte*, dan baris r=3 digeser sejarak 3 *byte.* Baris r=0 tidak digeser seperti gambar 7 berikut.



Gambar 7. Tranformasi *ShiftRows*

Hasil pergeseran pada proses *ShiftRows* dapat dilihat pada gambar 8 berikut.

6F	59	45	A4
72	76	C5	A4
63	C5	D4	AF
50	7B	C0	01

Gambar 8. Hasil Transformasi *ShiftRows*

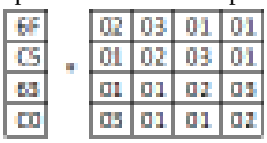
7. Transformasi *MixColumns*

Transformasi *MixColumns* adalah dengan mengalikan setiap kolom dari *array state* dengan matriks *MixColumns Rijndael* seperti gambar 9 berikut.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Gambar 9. Matriks *MixColums*

Transformasi *MixColumns* dinyatakan sebagai perkalian matriks seperti gambar 10 berikut.



Gambar 10. Transformasi *MixColumns*

a. Untuk mencari nilai pada baris satu kolom satu, konversi terlebih dahulu elemen matriks menjadi *binary digit*
   $6F_{16} = 01101111_2$
   $C5_{16} = 11000101_2$
   $63_{16} = 01100011_2$
   $C0_{16} = 11000000_2$
b. Melakukan perkalian *Galois Field* (2^8) dengan matriks *Rijndael (AES 128-Bit)* dengan mengalikan setiap baris elemen *array state* dengan kolom matriks.
   Ketentuan perkalian :
   1. Jika elemen *array state* dikali 01 maka hasilnya tidak berubah atau dikali 01.
   2. Jika elemen *array state* dikali 02 maka harus menggeser 1 *bit* elemen *binary digit* ke arah kiri.
   3. Jika elemen *array state* dikali 03 maka harus menggeser 1 *bit* elemen *binary digit* ke arah kiri, lalu melakukan operasi *XOR* dengan *array state* semula. Setelah itu melakukan operasi *XOR* dengan $[11B]_{16}$ atau $[100011011]_2$.

   Maka hasil perkalian *Galois Field* adalah sebagai berikut.

   $6F_{16}$ = $[01101111]_2$ x [02]
   = $[11011110]_2$
   = $[29]_{16}$

   $C5_{16}$ = $[11000101]_2$ x [03]
   = 1 1 0 0 0 1 0 1
   1 1 0 0 0 1 0 1 *XOR*

= 1 0 1 0 0 1 1 1 1
1 0 0 0 1 1 0 1 1 *XOR* dengan $[11B]_{16}$
0 0 1 0 1 0 1 0 0
$= [01010100]_2$
$= [54]_{16}$

$63_{16} = [01100011]_2 \times [01]$
$= [01100011]_2$
$= [63]_{16}$

$C0_{16} = [11000000]_2 \times [01]$
$= [11000000]_2$
$= [C0]_{16}$

Setelah melakukan perkalian *Galois Field,* selanjutnya melakukan operasi *XOR* pada setiap hasil *binary digit* setiap elemen *array state.*

1 1 0 1 1 1 1 0
0 1 0 1 0 1 0 0
0 1 1 0 0 0 1 1
1 1 0 0 0 0 0 0 *XOR*
0 0 1 0 1 0 0 1 = $[29]_{16}$

Hasil perkalian matriks *MixColumns* dengan *array state* dapat dilihat pada gambar 11 berikut.

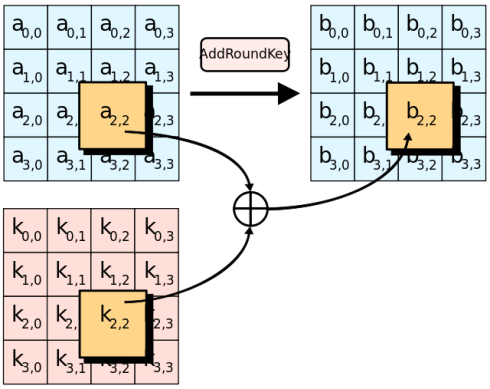
29	**81**	**98**	**1D**
9B	**5F**	**96**	**D9**
37	**6F**	**74**	**1A**
8C	**88**	**C9**	**D8**

Gambar 11. Hasil Tranformasi *MixColumns*

Untuk menemukan hasil dari baris dua kolom satu dan seterusnya, dapat melakukan operasi perkalian seperti di atas.

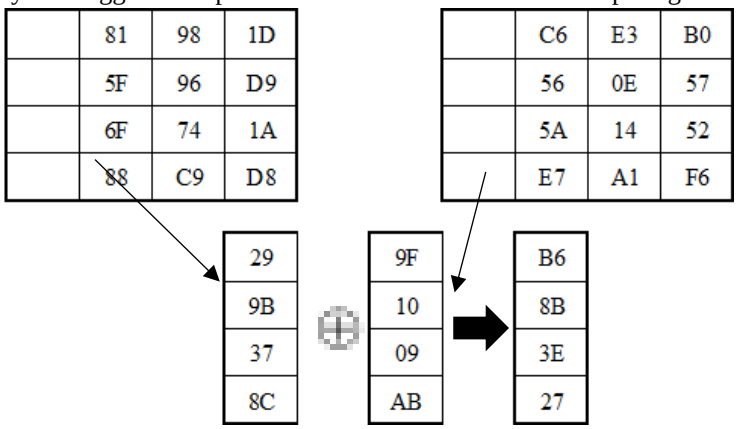
8. Transformasi *AddRoundKeys*

Transformasi ini melakukan operasi *XOR* terhadap sebuah *round key* dengan *array state*, dan hasilnya disimpan di *array state* seperti gambar 12 berikut.



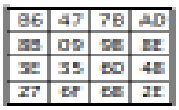
Gambar 12. Tranformasi *AddRoundKeys*

Baris satu kolom satu pada *array state* dilakukan operasi *XOR* dengan baris satu kolom satu pada *round key (Add Round Key)* dan seterusnya sehingga mendapatkan sebuah matriks berordo 4.4 seperti gambar 13 berikut.



Gambar 13. Proses Transformasi *Addroundkey* (Enkripsi)

Hasil keseluruhan transformasi *Addroundkey* dapat dilihat pada gambar 14 berikut.



Gambar 14. Hasil Transformasi *Addroundkey*

Keseluruhan proses enkripsi algoritma *AES 128-bit (Rijndael)* setelah melewati sepuluh putaran dan hasilnya dapat dilihat pada gambar 15 berikut.

Plaintext (input)				Key (input)				Ciphertext (output)			
53	4c	4d	4e	55	59	25	53	D6	5F	31	0B
45	41	45	47	4a	46	58	59	44	D0	1E	65
4b	48	4e	41	52	53	4e	46	41	96	EF	7F
4f	20	45	48	46	4c	46	57	56	73	77	AD

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 0													06	15	68	1D	55	59	25	53	
													0F	07	1D	1E	4A	46	58	59	
													19	1B	00	07	52	53	4E	46	
													09	6C	03	1F	46	4C	46	57	
Round 1	6F	59	45	A4	6F	59	45	A4	29	81	98	1D	B6	47	7B	AD	9F	C6	E3	B0	01
	76	C5	A4	72	C5	A4	72	76	9B	5F	96	D9	8B	09	98	8E	10	56	0E	57	
	D4	AF	63	C5	63	C5	D4	AF	37	6F	74	1A	3E	35	60	48	09	5A	14	52	
	01	50	7B	C0	C0	01	50	7B	8C	88	C9	D8	27	6F	68	2E	AB	E7	A1	F6	
Round 2	4E	A0	21	95	4E	A0	21	95	7E	0F	73	A5	B8	0F	90	F6	C6	00	E3	53	02
	3D	01	46	19	01	46	19	3D	16	16	76	0B	06	50	3E	14	10	46	48	1F	
	B2	96	D0	52	D0	52	B2	96	A7	0D	A4	50	EC	1C	A1	07	4B	11	05	57	
	CC	A8	45	31	31	CC	A8	45	61	6C	83	85	2D	C7	89	79	4C	AB	0A	FC	
Round 3	6C	76	60	42	6C	76	60	42	A9	3C	DD	0E	AB	3E	3C	BC	02	02	E1	B2	04
	6F	53	B2	FA	53	B2	FA	6F	2A	85	00	84	61	88	45	DE	4B	0D	45	5A	
	CE	9C	32	C5	32	C5	CE	9C	9A	26	4C	FC	61	CC	A3	44	FB	EA	EF	B8	
	D8	C6	A7	B6	B6	D8	C6	A7	A2	46	03	60	03	4C	03	9C	A1	0A	00	FC	
Round 4	62	B2	EB	65	62	B2	EB	65	47	AD	2C	D0	F3	1B	7B	35	B4	B6	57	E5	08
	EF	C4	6E	1D	C4	6E	1D	EF	31	38	D2	06	16	12	BD	33	27	2A	6F	35	
	EF	4B	0A	1B	0A	1B	EF	4B	CB	67	48	91	80	C6	06	67	4B	A1	4E	F6	
	7B	29	7B	DE	DE	7B	29	7B	CF	4E	86	FD	59	D2	1A	9D	96	9C	9C	60	
Round 5	0D	AF	21	96	0D	AF	21	96	6B	85	64	E8	59	01	B7	DE	32	84	D3	36	10
	47	C9	7A	C3	C9	7A	C3	47	6B	04	45	7D	0E	4B	65	68	65	4F	20	15	
	CD	B4	6F	85	6F	85	CD	B4	F8	82	A7	5F	63	B8	D3	DD	9B	3A	74	82	
	CB	B5	A2	5E	5E	CB	B5	A2	0D	98	1C	0D	42	4B	53	22	4F	D3	4F	2F	
Round 6	CB	7C	A9	1D	CB	7C	A9	1D	B6	C2	CE	5D	FD	0D	D2	77	4B	CF	1C	2A	20
	AB	B3	4D	45	B3	4D	45	AB	8F	92	86	09	F9	AB	9F	05	76	39	19	0C	
	FB	6C	66	C1	66	C1	FB	6C	1A	DC	CF	42	94	68	0F	00	8E	B4	C0	42	
	2C	B3	ED	93	93	2C	B3	ED	AE	50	23	21	E4	C9	F5	D8	4A	99	D6	F9	
Round 7	54	D7	B5	F5	54	D7	B5	F5	19	C9	33	E2	EC	F3	15	EE	F5	3A	26	0C	40
	99	62	DB	6B	62	DB	6B	99	6B	B6	D8	F5	31	D5	A2	83	5A	63	7A	76	
	22	45	76	63	76	63	22	45	79	71	E6	D7	6E	D2	85	F6	17	A3	63	21	
	69	DD	E6	61	61	69	DD	E6	2A	08	2C	0F	85	3E	CC	16	AF	36	E0	19	
Round 8	CE	0D	59	28	CE	0D	59	28	52	81	B0	FC	1F	F6	E1	A1	4D	77	51	5D	80
	C7	03	3A	EC	03	3A	EC	C7	2D	28	92	32	8A	EC	2C	FA	A7	C4	BE	C8	
	9F	B5	97	42	97	42	9F	B5	31	11	5D	43	F2	71	5E	61	C3	60	03	22	
	97	B2	4B	47	47	97	B2	4B	53	5A	E7	9C	02	3D	60	02	51	67	87	9E	
Round 9	C0	42	F8	32	C0	42	F8	32	FD	8F	32	95	43	46	AA	50	BE	C9	98	C5	1B
	7E	CE	71	2D	CE	71	2D	7E	D8	FD	05	E0	EC	0D	4B	66	34	F0	4E	86	
	89	A3	58	EF	58	EF	89	A3	27	6F	B5	7A	EF	C7	1E	F3	C8	A8	AB	89	
	77	27	D0	77	77	77	27	D0	23	B6	F9	30	3E	CC	04	53	1D	7A	FD	63	
Round 10	1A	5A	AC	53	1A	5A	AC	53					D6	5F	31	0B	CC	05	9D	58	36
	CE	D7	B3	33	D7	B3	33	CE					44	D0	1E	65	93	63	2D	AB	
	DF	C6	72	0D	72	0D	DF	C6					41	96	EF	7F	33	9B	30	B9	
	B2	4B	F2	ED	ED	B2	4B	F2					56	73	77	AD	BB	C1	3C	5F	
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Gambar 15. Keseluruhan Proses Enkripsi Algoritma *Rijndael*

9. Konversi Heksadesimal

Hasil transformasi enkripsi keseluruhan dikonversi menjadi huruf alfabet untuk mengetahui hasil setelah dienkripsi seperti berikut.

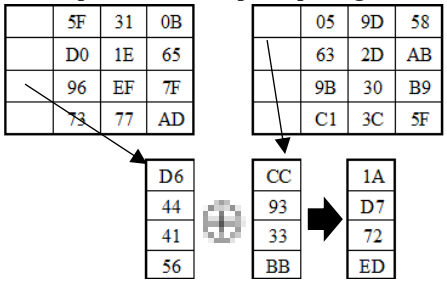
D6 44 41 56 5F D0 96 73 31 1E EF 77 0B 65 7F AD

Ö D A V _ Đ – s 1 RS ï w VT e DEL SPASI

Untuk mengetahui pesan yang telah dienkripsi maka dilakukan proses dekripsi. Proses dekripsi suatu plainteks dengan kombinasi algoritma *Rijndael (AES 128-Bit)* dengan *Caesar Cipher* terdiri dari beberapa jenis yaitu *Addroundkey*, *InvMixColumns*, *InvShiftRows*, dan *InvSubbytes.*

1. *AddRoundkey*

   Transformasi *AddRoundKey* adalah dengan melakukan proses *XOR* antara *ciphertext* dengan *roundkey* dimulai dari urutan *roundkey* ke sepuluh yang digunakan pada saat enkripsi seperti gambar 16 berikut.



Gambar 16. Proses Transformasi *AddRoundKey* (Dekripsi)

Hasil keseluruhan transformasi *AddRoundKey* dapat dilihat pada gambar 17 berikut.

1A	5A	AC	53
D7	B3	33	CE
72	0D	DF	C6
ED	B2	4B	F2

Gambar 17. Hasil Keseluruhan *AddRoundkey* (Dekripsi)

2. *InvMixColumns*

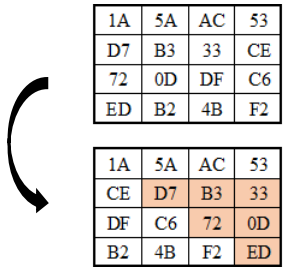
   Transformasi *InvMixColumns* sama dengan *MixColumns*, dimana perbedaannya adalah a(x) yang digunakan adalah invers $a^{-1}(x)$ dan digunakan matriks *InvMixColumns Rijndael* seperti gambar 18 berikut.

$$\begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix}$$

Gambar 18. Matriks *InvMixColumns Rijndael*

3. *InvShiftRows*

   Proses *InvShiftRows* adalah kebalikan dari proses *ShiftRows* dimana proses pergeseran baris dari *array state* dimulai dari baris paling bawah seperti gambar 19 berikut.



Gambar 19. Proses Transformasi *InvShiftRows*

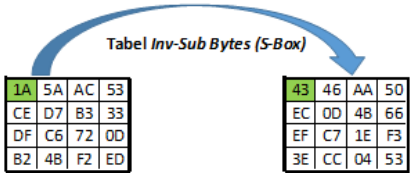
4. *InvSubbytes*

   Proses *InvSubBytes* sama dengan proses transformasi *SubBytes*, namun tabel yang digunakan berbeda. Tabel yang digunakan pada proses ini adalah tabel *Invers S-Box Rijndael* yang dapat dilihat pada gambar 20 berikut.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 20. *Invers S-Box Rijndael*

Tahapan pensubstitusian adalah sebagai berikut : Jika setiap *byte* pada *array state* S[rows, columns] = xy, dengan xy adalah digit heksadesimal dari nilai S[r,c] maka nilai substitusinya dinyatakan dengan S'[r,c] yaitu elemen di dalam *S-Box* yang merupakan perpotongan baris x dengan kolom y seperti gambar 21 berikut.



Gambar 21. Hasil *InvSubBytes*

Hasil keseluruhan proses dekripsi *ciphertext* dengan kombinasi algoritma *Rijndael (AES 128-Bit)* dan *Caesar Cipher* setelah melewati sepuluh *round inverse* adalah seperti gambar 22 berikut.

53	4C	4D	4E
45	41	45	47
4B	48	4E	41
4F	20	45	48

Gambar 22. Hasil dekripsi keseluruhan

Keseluruhan proses dekripsi algoritma *AES 128-bit (Rijndael)* dapat dilihat pada gambar 23 berikut.

Ciphertext (input)				Key (input)				Plaintext (output)			
D6	5F	31	0B	55	59	25	53	53	4C	4D	4E
44	D0	1E	65	4a	46	58	59	45	41	45	47
41	96	EF	7F	52	53	4e	46	4B	48	4E	41
56	73	77	AD	46	4c	46	57	4F	20	45	48

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 0													53	4C	4D	4E	55	59	25	53	
													45	41	45	47	4A	46	58	59	
													4B	48	4E	41	52	53	4E	46	
													4F	20	45	48	46	4C	46	57	
Round 1	06	15	68	1D	6F	59	45	A4	6F	59	45	A4	29	81	98	1D	9F	C6	E3	B0	01
	0F	07	1D	1E	76	C5	A4	72	C5	A4	72	76	9B	5F	96	D9	10	56	0E	57	
	19	1B	00	07	D4	AF	63	C5	63	C5	D4	AF	37	6F	74	1A	09	5A	14	52	
	09	6C	03	1F	01	50	7B	C0	C0	01	50	7B	8C	88	C9	D8	AB	E7	A1	F6	
Round 2	B6	47	7B	AD	4E	A0	21	95	4E	A0	21	95	7E	0F	73	A5	C6	00	E3	53	02
	8B	09	98	8E	3D	01	46	19	01	46	19	3D	16	16	76	0B	10	46	48	1F	
	3E	35	60	48	B2	96	D0	52	D0	52	B2	96	A7	0D	A4	50	4B	11	05	57	
	27	6F	68	2E	CC	A8	45	31	31	CC	A8	45	61	6C	83	85	4C	AB	0A	FC	
Round 3	B8	0F	90	F6	6C	76	60	42	6C	76	60	42	A9	3C	DD	0E	02	02	E1	B2	04
	06	50	3E	14	6F	53	B2	FA	53	B2	FA	6F	2A	85	00	84	4B	0D	45	5A	
	EC	1C	A1	07	CE	9C	32	C5	32	C5	CE	9C	9A	26	4C	FC	FB	EA	EF	B8	
	2D	C7	89	79	D8	C6	A7	B6	B6	D8	C6	A7	A2	46	03	60	A1	0A	00	FC	
Round 4	AB	3E	3C	BC	62	B2	EB	65	62	B2	EB	65	47	AD	2C	D0	B4	B6	57	E5	08
	61	88	45	DE	EF	C4	6E	1D	C4	6E	1D	EF	31	38	D2	06	27	2A	6F	35	
	61	CC	A3	44	EF	4B	0A	1B	0A	1B	EF	4B	CB	67	48	91	4B	A1	4E	F6	
	03	4C	03	9C	7B	29	7B	DE	DE	7B	29	7B	CF	4E	86	FD	96	9C	9C	60	
Round 5	F3	1B	7B	35	0D	AF	21	96	0D	AF	21	96	6B	85	64	E8	32	84	D3	36	10
	16	12	BD	33	47	C9	7A	C3	C9	7A	C3	47	6B	04	45	7D	65	4F	20	15	
	80	C6	06	67	CD	B4	6F	85	6F	85	CD	B4	F8	82	A7	5F	9B	3A	74	82	
	59	D2	1A	9D	CB	B5	A2	5E	5E	CB	B5	A2	0D	98	1C	0D	4F	D3	4F	2F	
Round 6	59	01	B7	DE	CB	7C	A9	1D	CB	7C	A9	1D	B6	C2	CE	5D	4B	CF	1C	2A	20
	0E	4B	65	68	AB	B3	4D	45	B3	4D	45	AB	8F	92	86	09	76	39	19	0C	
	63	B8	D3	DD	FB	6C	66	C1	66	C1	FB	6C	1A	DC	CF	42	8E	B4	C0	42	
	42	4B	53	22	2C	B3	ED	93	93	2C	B3	ED	AE	50	23	21	4A	99	D6	F9	
Round 7	FD	0D	D2	77	54	D7	B5	F5	54	D7	B5	F5	19	C9	33	E2	F5	3A	26	0C	40
	F9	AB	9F	05	99	62	DB	6B	62	DB	6B	99	6B	B6	D8	F5	5A	63	7A	76	
	94	68	0F	00	22	45	76	63	76	63	22	45	79	71	E6	D7	17	A3	63	21	
	E4	C9	F5	D8	69	DD	E6	61	61	69	DD	E6	2A	08	2C	0F	AF	36	E0	19	
Round 8	EC	F3	15	EE	CE	0D	59	28	CE	0D	59	28	52	81	B0	FC	4D	77	51	5D	80
	31	D5	A2	83	C7	03	3A	EC	03	3A	EC	C7	2D	28	92	32	A7	C4	BE	C8	
	6E	D2	85	F6	9F	B5	97	42	97	42	9F	B5	31	11	5D	43	C3	60	03	22	
	85	3E	CC	16	97	B2	4B	47	47	97	B2	4B	53	5A	E7	9C	51	67	87	9E	
Round 9	1F	F6	E1	A1	C0	42	F8	32	C0	42	F8	32	FD	8F	32	95	BE	C9	98	C5	1B
	8A	EC	2C	FA	7E	CE	71	2D	CE	71	2D	7E	D8	FD	05	E0	34	F0	4E	86	
	F2	71	5E	61	89	A3	58	EF	58	EF	89	A3	27	6F	B5	7A	C8	A8	AB	89	
	02	3D	60	02	77	27	D0	77	77	77	27	D0	23	B6	F9	30	1D	7A	FD	63	
Round 10	43	46	AA	50	1A	5A	AC	53					1A	5A	AC	53	CC	05	9D	58	36
	EC	0D	4B	66	CE	D7	B3	33					D7	B3	33	CE	93	63	2D	AB	
	EF	C7	1E	F3	DF	C6	72	0D					72	0D	DF	C6	33	9B	30	B9	
	3E	CC	04	53	B2	4B	F2	ED					ED	B2	4B	F2	BB	C1	3C	5F	
																	Key Schedule				Round Constant

Gambar 22. Keseluruhan Proses Dekripsi Algoritma *AES-128* Bit

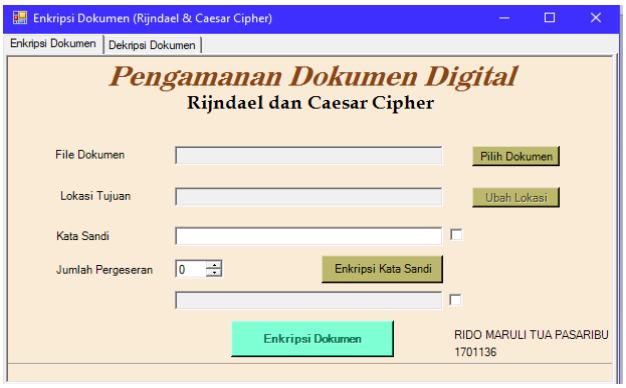
 https://doi.org/10.56211/helloworld.v1i1.11

5. Konversi Heksadesimal
   Setelah selesai keseluruhan proses dekripsi menggunakan algoritma *Rijndael*, maka akan dikonversikan ke bentuk plainteks untuk melihat dalam bentuk karakter alfabet.
   53 45 4B 4F 4C 41 48 20 4D 45 4E 45 4E 47 41 48
   S E K O L A H SPASI M E N E N G A H

Hasil Percobaan

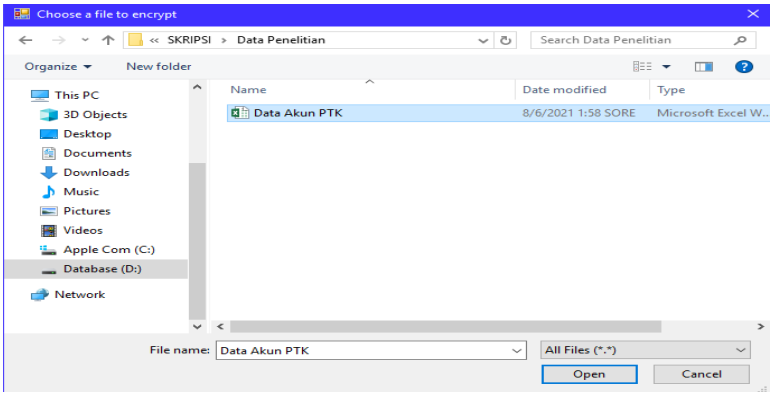
Sistem pengamanan dokumen digital yang telah dirancang selanjutnya dilanjutkan ke tahap implementasi algoritma *Rijndael (AES 128-Bit)* dan *Caesar Cipher* pada aplikasi.

1. Form Tampilan Enkripsi
   Form Tampilan enkripsi berisikan menu-menu yang dapat dibuka oleh *user*. Pada *Form* Tampilan enkripsi akan ditampilkan menu-menu pilihan dijalankan oleh *user*. Tampilan halaman enkripsi dapat dilihat pada gambar 23 berikut.



Gambar 23. Tampilan Enkripsi *Rijndael* dan *Caesar Cipher*

2. Form Pencarian Dokumen Digital yang akan Dienkripsi
   Form Pencarian berisikan komponen-komponen untuk pencarian dokumen digital sehingga *user* dapat mencari pada kotak dialog. Setelah selesai memilih maka akan tampil nama *file* dan tipe *file* yang dipilih seperti "Data Akun PTK.xlxs" pada folder "Data Penelitian", lalu pilih *file* untuk mengenkripsi seperti pada gambar 24 berikut.



Gambar 24. Tampilan Pencarian *File* Enkripsi

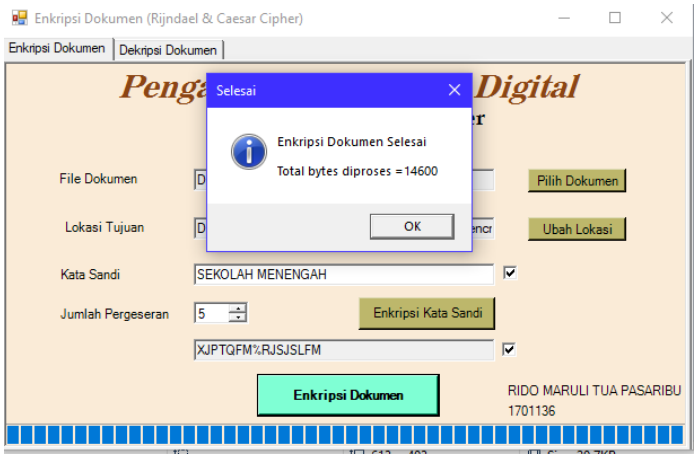
3. Form Enkripsi *Key* dengan *Caesar Cipher*
   Setelah pencarian *file* telah selesai, maka akan muncul tampilan seperti gambar 25 berikut.

Gambar 25. Tampilan Enkripsi *Key* dengan *Caesar Cipher*

Gambar 25 menunjukkan lokasi *file* yang terpilih yang berada pada *folder* Data Penelitian. Pada *form* ini *user* mengisikan *key* dan jumlah pergeseran dengan *Caesar Cipher*. Kemudian mengklik enkripsi kata sandi, maka akan tampil *Key* yang sudah dienkripsi dengan *Caesar Cipher*. Setelah *Key* sudah dienkripsi maka *user* dapat mengklik enkripsi dokumen untuk memproses enkripsi dengan algoritma *Rijndael* (*AES 128-Bit).*

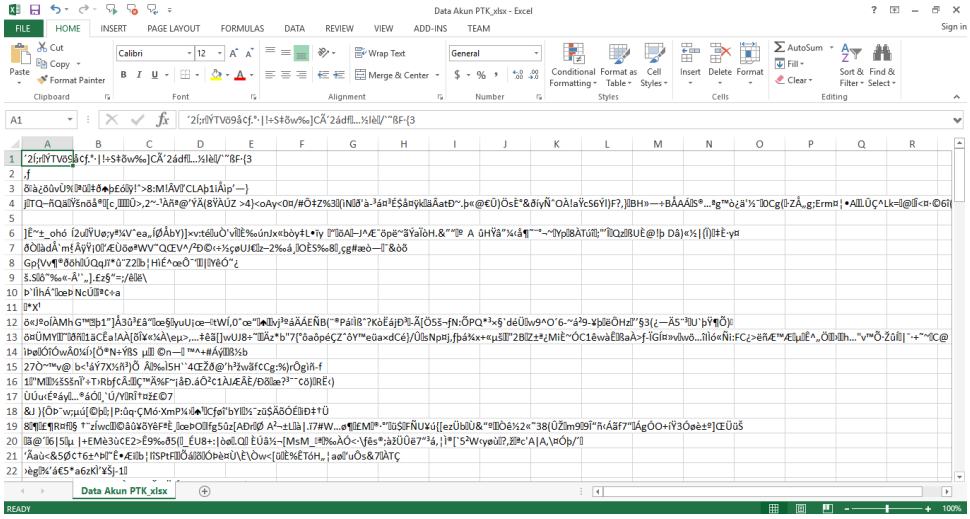
4. Hasil Enkripsi

Setelah proses enkripsi selesai maka akan muncul *pop-up* yang menampilkan enkripsi telah selesai seperti gambar 26 berikut.



Gambar 26. Tampilan Selesai Enkripsi *Rijndael* dan *Caesar Cipher*

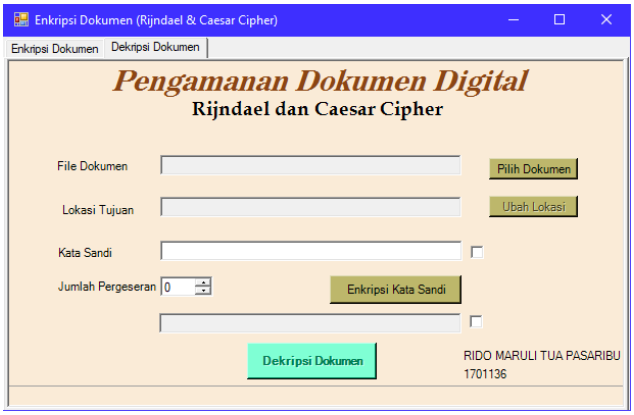
Setelah proses enkripsi berhasil *output* aplikasi ini berupa informasi atau *ciphertext* yang telah berubah, yang dapat dilihat pada gambar 27 berikut.



Gambar 27. Tampilan Enkripsi Data Akun PTK

5. Form Tampilan Dekripsi

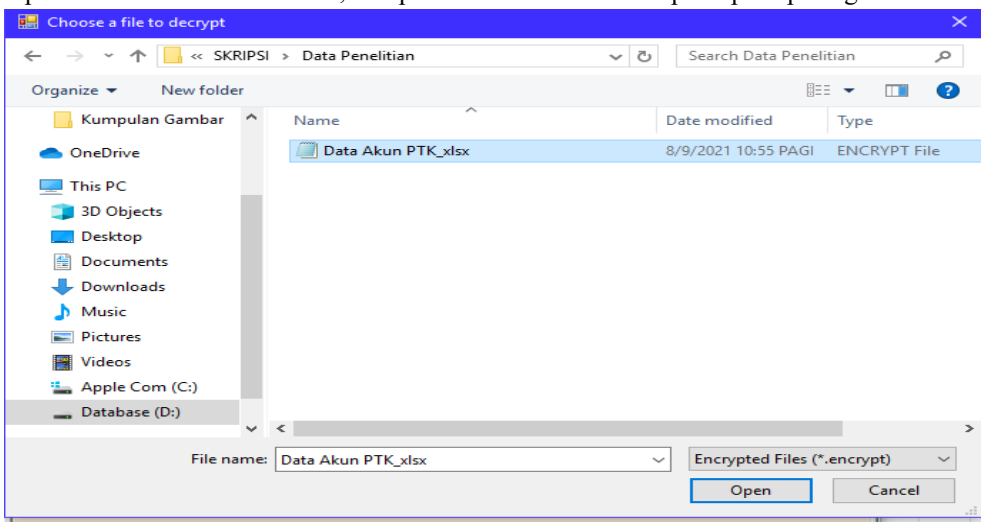
Form tampilan dekripsi berisikan menu-menu yang dapat dibuka oleh *user.* Pada *Form* tampilan dekripsi akan ditampilkan menu-menu pilihan dijalankan oleh *user*. Tampilan halaman dekripsi dapat dilihat pada gambar 28 berikut.



Gambar 28. Tampilan Dekripsi *Rijndael* dan *Caesar Cipher*

6. Form Pencarian Dokumen Digital yang akan Didekripsi

   Form Pencarian berisikan komponen-komponen untuk pencarian dokumen digital sehingga user dapat mencari pada kotak dialog. Setelah selesai memilih maka akan tampil nama file dan tipe file yang dipilih seperti "Data Akun PTK.encrypt" pada folder "Data Penelitian", lalu pilih file untuk mendekripsi seperti pada gambar 29 berikut.



Gambar 29. Tampilan Pencarian *File* Dekripsi

7. Form Dekripsi *Key* dengan *Caesar Cipher*

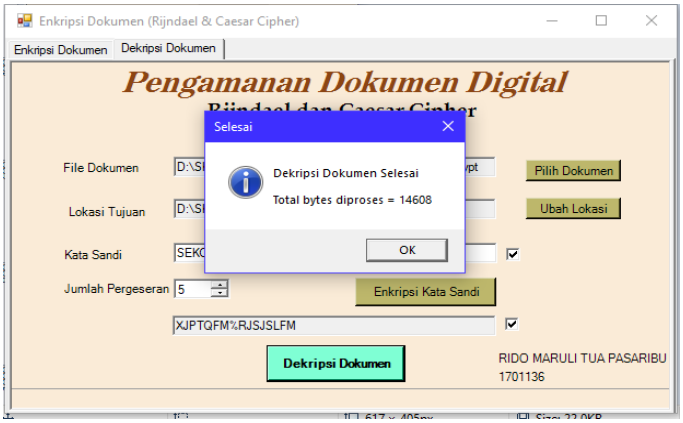
   Setelah pencarian file telah selesai, maka akan muncul tampilan seperti gambar 30 berikut.

Gambar 30. Tampilan Dekripsi *Key* dengan *Caesar Cipher*

Gambar 30 menunjukkan lokasi file yang terpilih yang berada pada folder Data Penelitian. Pada form ini user mengisikan *key* dan jumlah pergeseran dengan *Caesar Cipher*. Kemudian mengklik enkripsi kata sandi, maka akan tampil *key* yang sudah dienkripsi dengan *Caesar Cipher*. Setelah *key* sudah dienkripsi maka user dapat mengklik dekripsi dokumen untuk memproses dekripsi dengan algoritma *Rijndael (AES 128-Bit).*

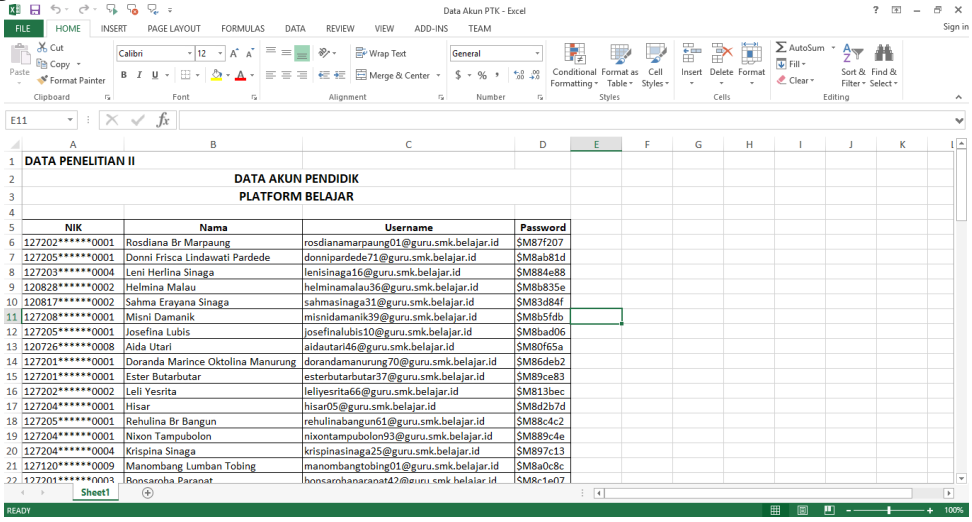
8. Hasil Dekripsi

   Setelah proses dekripsi selesai maka akan muncul *pop-up* yang menampilkan dekripsi telah selesai seperti gambar 31 berikut.



Gambar 31. Tampilan Selesai Dekripsi *Rijndael* dan *Caesar Cipher*

Setelah proses dekripsi berhasil *output* aplikasi ini berupa informasi atau *Plaintext* yang telah berubah, yang dapat dilihat pada gambar 32 berikut.



Data Akun PTK - Excel

DATA PENELITIAN II

DATA AKUN PENDIDIK
PLATFORM BELAJAR

NIK	Nama	Username	Password
127202******0001	Rosdiana Br Marpaung	rosdianamarpaung01@guru.smk.belajar.id	$M87f207
127205******0001	Donni Frisca Lindawati Pardede	donnipardede71@guru.smk.belajar.id	$M8ab81d
127203******0004	Leni Herlina Sinaga	lenisinaga16@guru.smk.belajar.id	$M884e88
120828******0002	Helmina Malau	helminamalau36@guru.smk.belajar.id	$M8b835e
120817******0002	Sahma Erayana Sinaga	sahmasinaga31@guru.smk.belajar.id	$M83d84f
127208******0001	Misni Damanik	misnidamanik39@guru.smk.belajar.id	$M8b5fdb
127205******0001	Josefina Lubis	josefinalubis10@guru.smk.belajar.id	$M8bad06
120726******0008	Aida Utari	aidautari46@guru.smk.belajar.id	$M80f65a
127201******0001	Doranda Marince Oktolina Manurung	dorandamanurung70@guru.smk.belajar.id	$M86deb2
127201******0001	Ester Butarbutar	esterbutarbutar37@guru.smk.belajar.id	$M89ce83
127202******0002	Leli Yesrita	leliyesrita66@guru.smk.belajar.id	$M813bec
127204******0001	Hisar	hisar05@guru.smk.belajar.id	$M8d2b7d
127205******0001	Rehulina Br Bangun	rehulinabangun61@guru.smk.belajar.id	$M88c4c2
127204******0001	Nixon Tampubolon	nixontampubolon93@guru.smk.belajar.id	$M889c4e
127204******0004	Krispina Sinaga	krispinasinaga25@guru.smk.belajar.id	$M897c13
127120******0009	Manombang Lumban Tobing	manombangtobing01@guru.smk.belajar.id	$M8a0c8c
127201******0003	Bonsaroha Parapat	bonsarohaparapat42@guru.smk.belajar.id	$M8c1e07

Gambar 32. Tampilan Dekripsi Data Akun PTK

KESIMPULAN DAN SARAN

Setelah selesai dilakukan analisis, perancangan serta implementasi menggunakan algoritma Rijndael (AES 128-Bit) dan Caesar Cipher dapat ditarik kesimpulan bahwa dengan adanya sistem keamanan dokumen digital pada SMK Negeri 3 Pematangsiantar dapat terbantu dalam mencegah cyber crime dan mengamankan data-data yang bersifat rahasia di SMK Negeri 3 Pematangsiantar. Hasil enkripsi merupakan sekumpulan kombinasi karakter yang tidak dapat dimengerti oleh manusia. Untuk hasil enkripsi akan selalu sama dengan hasil dekripsi dengan menggunakan key yang sama. Adapun beberapa saran yang dapat diberikan diantaranya bahwa penelitian ini dapat dikembangkan dengan mengkombinasikan algoritma lain seperti Blowfish, Mars dan lainnya. Selain itu aplikasi dapat dikembangkan berbasis online sehingga dapat digunakan banyak user sehingga meningkatkan efisiensi.

DAFTAR PUSTAKA

[1] F. Mahbub, M. Syahrizal, and R. K. Hondro, "Modifikasi Kunci Algoritma IDEA Menggunakan Random Key Midsquare Pada Citra," *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 4, no. 1, pp. 204–210, 2020.

[2] R. Sartika, S. A. I. Siregar, and N. P. R. K. Sari, "Kekhususan Proses Penyidikan Tindak Pidana Cyber Crime," *Jurnal Aktual Justice*, vol. 5, no. 1, pp. 38–55, 2020.

[3] P. P. P. A. N. . F. I. R.H Zer, Masitha, A. P. Windarto, and A. Wanto, "Analysis of the ELECTRE Method on the Selection of Student Creativity Program Proposals," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–7, 2019.

[4] A. P. W. Budiharjo and A. Muhammad, "Comparison of Weighted Sum Model and Multi Attribute Decision Making Weighted Product Methods in Selecting the Best Elementary School in Indonesia," *International Journal of Software Engineering and Its Applications*, vol. 11, no. 4, pp. 69–90, 2017.

[5] D. R. Sari, N. Rofiqo, D. Hartama, A. P. Windarto, and A. Wanto, "Analysis of the Factors Causing Lazy Students to Study Using the ELECTRE II Algorithm," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.

[6] K. Fatmawati *et al.*, "Analysis of Promothee II Method in the Selection of the Best Formula for Infants Under Three Years," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, Aug. 2019.

[7] P. Alkhairi, L. P. Purba, A. Eryzha, A. P. Windarto, and A. Wanto, "The Analysis of the ELECTREE II Algorithm in Determining the Doubts of the Community Doing Business Online," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–7, 2019.

[8] S. Sundari, Karmila, M. N. Fadli, D. Hartama, A. P. Windarto, and A. Wanto, "Decision Support System on Selection of Lecturer Research Grant Proposals using Preferences Selection Index," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–7, 2019.

[9] S. R. Ningsih, R. Wulansari, D. Hartama, A. P. Windarto, and A. Wanto, "Analysis of PROMETHEE II Method on Selection of Lecturer Community Service Grant Proposals," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–7, 2019.

[10] T. Imandasari, M. G. Sadewo, A. P. Windarto, A. Wanto, H. O. Lingga Wijaya, and R. Kurniawan, "Analysis of the Selection Factor of Online Transportation in the VIKOR Method in Pematangsiantar City," *Journal of*

Physics: Conference Series, vol. 1255, no. 1, pp. 1–7, 2019.
[11] E. Siregar, H. Mawengkang, E. B. Nababan, and A. Wanto, "Analysis of Backpropagation Method with Sigmoid Bipolar and Linear Function in Prediction of Population Growth," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[12] G. W. Bhawika *et al.*, "Implementation of ANN for Predicting the Percentage of Illiteracy in Indonesia by Age Group," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[13] W. Saputra, J. T. Hardinata, and A. Wanto, "Resilient method in determining the best architectural model for predicting open unemployment in Indonesia," *IOP Conference Series: Materials Science and Engineering*, vol. 725, no. 1, pp. 1–7, 2020.
[14] A. Wanto and J. T. Hardinata, "Estimations of Indonesian poor people as poverty reduction efforts facing industrial revolution 4.0," *IOP Conference Series: Materials Science and Engineering*, vol. 725, no. 1, pp. 1–8, 2020.
[15] A. Wanto *et al.*, "Model of Artificial Neural Networks in Predictions of Corn Productivity in an Effort to Overcome Imports in Indonesia," *Journal of Physics: Conference Series*, vol. 1339, no. 1, pp. 1–6, 2019.
[16] A. Wanto *et al.*, "Analysis of the Accuracy Batch Training Method in Viewing Indonesian Fisheries Cultivation Company Development," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[17] I. S. Purba *et al.*, "Accuracy Level of Backpropagation Algorithm to Predict Livestock Population of Simalungun Regency in Indonesia," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[18] P. Parulian *et al.*, "Analysis of Sequential Order Incremental Methods in Predicting the Number of Victims Affected by Disasters," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[19] A. Wanto *et al.*, "Analysis of the Backpropagation Algorithm in Viewing Import Value Development Levels Based on Main Country of Origin," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[20] S. Setti, A. Wanto, M. Syafiq, A. Andriano, and B. K. Sihotang, "Analysis of Backpropagation Algorithms in Predicting World Internet Users," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[21] T. Afriliansyah *et al.*, "Implementation of Bayesian Regulation Algorithm for Estimation of Production Index Level Micro and Small Industry," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[22] A. Wanto *et al.*, "Forecasting the Export and Import Volume of Crude Oil , Oil Products and Gas Using ANN," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[23] M. K. Z. Sormin, P. Sihombing, A. Amalia, A. Wanto, D. Hartama, and D. M. Chan, "Predictions of World Population Life Expectancy Using Cyclical Order Weight / Bias," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–6, 2019.
[24] R. Rahim *et al.*, "C4.5 Classification Data Mining for Inventory Control," *International Journal of Engineering & Technology*, vol. 7, pp. 68–72, 2018.
[25] I. Parlina *et al.*, "Naive Bayes Algorithm Analysis to Determine the Percentage Level of visitors the Most Dominant Zoo Visit by Age Category," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–5, 2019.
[26] I. S. Damanik, A. P. Windarto, A. Wanto, Poningsih, S. R. Andani, and W. Saputra, "Decision Tree Optimization in C4.5 Algorithm Using Genetic Algorithm," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–7, 2019.
[27] H. Siahaan, H. Mawengkang, S. Efendi, A. Wanto, and A. Perdana Windarto, "Application of Classification Method C4.5 on Selection of Exemplary Teachers," in *Journal of Physics: Conference Series*, 2019, vol. 1235, no. 1, pp. 1–7.
[28] D. Hartama, A. Perdana Windarto, and A. Wanto, "The Application of Data Mining in Determining Patterns of Interest of High School Graduates," *Journal of Physics: Conference Series*, vol. 1339, no. 1, pp. 1–6, 2019.
[29] M. Widyastuti, A. G. Fepdiani Simanjuntak, D. Hartama, A. P. Windarto, and A. Wanto, "Classification Model C.45 on Determining the Quality of Custumer Service in Bank BTN Pematangsiantar Branch," *Journal of Physics: Conference Series*, vol. 1255, no. 012002, pp. 1–6, 2019.
[30] W. Katrina, H. J. Damanik, F. Parhusip, D. Hartama, A. P. Windarto, and A. Wanto, "C.45 Classification Rules Model for Determining Students Level of Understanding of the Subject," *Journal of Physics: Conference Series*, vol. 1255, no. 1, pp. 1–7, 2019.
[31] S. Sudirman, A. P. Windarto, and A. Wanto, "Data Mining Tools | RapidMiner : K-Means Method on Clustering of Rice Crops by Province as Efforts to Stabilize Food Crops In Indonesia," *IOP Conference Series: Materials Science and Engineering*, vol. 420, no. 012089, pp. 1–8, 2018.
[32] F. Achmad and E. R. Agustina, "Perancangan Spesifikasi Keamanan Kontrol Akses pada Aplikasi Layanan Informasi di Lingkungan Instansi Pemerintah," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 2, pp. 195–200, 2019.
[33] K. Y. Prasetyo, F. Damayanti, A. Basith, U. M. Wiji, R. F. Abdillah, and Khairunnisa, "Pengaruh E-Commerce terhadap Tindak Kejahatan Siber di Era Milenium untuk Generasi Milenial Kevin," *Journal of Education and Technology*, vol. 1, no. 2, pp. 81–86, 2021.
[34] M. Fahri H Damanik, Indra Gunawan, Zulaini Masruro Nasution, Sumarno, and Ika Okta Kirana, "Pemanfaatan Algoritma Aes Untuk Keamanann Data Karyawan Pt. Telkom Indonesia Pematangsiantar," *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 1, no. 1, pp. 32–37, 2022.
[35] D. A. Subandi Subandi, Basuki Hari Prasetyo, "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman Wahyu," *Jurnal Bit*, vol. 17, no. 2, pp. 46–52, 2020.

[36] E. E. Awal *et al.*, "Jurnal Mahasiswa Ilmu Komputer (JMIK) Jurnal Mahasiswa Ilmu Komputer (JMIK)," *Jurnal Mahasiswa Ilmu Komputer (JMIK)*, vol. 03, no. 01, pp. 260–265, 2022.
[37] I. M. Yusup, C. Carudin, and I. Purnamasari, "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 6, no. 3, pp. 434–441, 2020.
[38] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," *KAKIFIKOM (Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer)*, vol. 02, no. 01, pp. 31–42, 2020.

BIODATA PENULIS

Rido Maruli Tua Pasaribu
Alumni Mahasiswa STIKOM Tunas Bangsa, Pematangsiantar, Indonesia.
micaryus20@gmail.com

Rafiqa Dewi
rafiqa@amiktunasbangsa.ac.id
Dosen STIKOM Tunas Bangsa, Pematangsiantar, Indonesia.
rafiqa@amiktunasbangsa.ac.id

Iin Parlina
Dosen STIKOM Tunas Bangsa, Pematangsiantar, Indonesia.
iin@amiktunasbangsa.ac.id