E-ISSN : 2685 - 4902
Vol.1, No.02, November 2019

JURNAL ILMIAH
INTECH

Information Technology Journal of UMUS

EISSN : 2685-4902
Vol.1, No.02, November 2019

Jurnal Ilmiah

INTECH

Information Technology Journal of UMUS

Vol.1, No.02 November 2019
Jurnal Ilmiah INTECH: Information Technology Journal of UMUS

Terbit dua kali dalam setahun, yaitu pada bulan Mei dan November. Jurnal ini berisi artikel hasil pemikiran di bidang teknik informatika, teknik komputer, sistem informasi, dan jaringan komputer. Jurnal Ilmiah INTECH terbit pertama kali pada bulan Mei 2019

EDITOR IN CHIEF
Otong Saeful Bachri, S.Kom., M.Kom

MANAGING EDITOR
Harliana, ST., M.Cs

PRINCIPAL CONTACT
Nike Setiati, A.Md.Kom

SUPPORT CONTACT
Arif Wicaksono, S.A.P

MITRA BESTARI (STAFF AHLI)
Dr. Hamdani, ST., M.Cs (Universitas Mulawarman – Kalimantan Timur)
Heru Ismanto, S.Si., M.Cs (Universitas Merauke – Merauke Papua)
Hartatik, ST., M.Cs (Universitas AMIKOM Yogyakarya – Yogyakarta)
Andri Syafrianto, M.Cs (STMIK El Rahma – Yogyakarta)

PENANGGUNGJAWAB :
Rektor Universitas Muhadi Setiabudi Brebes: Dr. Robby Setiadi, S.Kom., M.M

ALAMAT PENYUNTING:
Program Studi Teknik Informatika, Universitas Muhadi Setiabudi Brebes.
Jalan Pangeran Diponogoro KM 2 Wanasari Brebes – Jawa Tengah 52252. Telp (0283) 6199000

Jurnal Ilmiah
INTECH
Information Technology Journal of UMUS

KATA PENGANTAR

Assalamualaikum Wr, Wb

Puji syukur kehadirat Allah SWT atas anugrahnya sehingga jurnal edisi kali ini dapat terbit. Sebelumnya kami ingin mengucapkan terimakasih banyak kepada dosen/peneliti/profesi yang telah mengirimkan artikelnya kepada dewan redaksi untuk dapat dipublish pada jurnal yang kami kelola. Semua artikel yang masuk kepada dewan redaksi telah melalui proses review oleh mitra bestari dan tim dewan redaksi, segala proses revisi dan redaksional juga telah dilakukan oleh penulis sebelum jurnal ini diterbitkan. Segala bentuk kritik dan saran yang membangun dari pembaca / peneliti yang dikirimkan sangat kami harapkan demi melakukan pembenahan jurnal yang kami kelola. Akhir kata kami menghaturkan terimakasih banyak kepada semua pihak yang sudah terlibat dalam proses penerbitan jurnal ini.

Wassalamualaikum wr wb.

Ketua Dewan Redaksi

DAFTAR ISI

IMPLEMENTASI KRIPTOGRASI AES DALAM PENGAMANAN DATA SELEKSI PESERTA JAMKESMAS

Susi Widyastuti*[1], Wahyu Ariandi[2], Vergamana Sulistiono[3]
[1,2,3]Program Studi Teknik Informatika, STIKOM Poltek Cirebon, Indonesia
e-mail: ***[1]miss_siwy@gmail.com** , [2]wahyuariandi@mail.ugm.ac.id,
[3]vergamana.sulistiono@gmail.com

Abstrak

Seiring perkembangan zaman, kemajuan teknologi komputer dan telekomunikasi telah menjadi kebutuhan yang sangat membantu dalam menyelesaikan banyak pekerjaan dengan cepat, tepat dan akurat. Tetapi ada juga dampak negative berupa penyadapan data-data penting oleh orang yang tidak berwenang/ berhak, sehingga aspek keamanan data dianggap penting untuk suatu informasi yang bersifat rahasia. Kriptografi merupakan salah satu dari solusi atau metode pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, serta dapat meningkatkan aspek keamanan suatu data atau informasi. Kriptografi merupakan bidang ilmu yang mempelajari tentang teknik penyandian data.kriptografi dibagi menjadi dua jenis yaitu klasik dan modern, serta memiliki kunci simetris dan asimetris. Pada kunci simetris terdapat Advanced Encrypstion Standard (AES) atau bisa juga disebut Rijndael. AES merupakan algoritma chipper yang aman untuk melindungi data atau informasi yang bersifat rahasia dengan menggunakan teknik enkripsi dan dekripsi dengan panjang kunci yang bervariasi, yaitu 128bit, 192bit dan 256bit. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi

Kata kunci*—Data penting, kriptografi, Advanced Encrypstion Standard (AES)*

Abstract

Along with the times, advances in computer and telecommunications technology have become a necessity that is very helpful in completing many jobs quickly, precisely and accurately. But there are also negative impacts in the form of tapping important data by people who are not authorized / entitled, so that the aspect of data security is considered important for confidential information. Cryptography is one of the solutions or methods for securing data that is appropriate for maintaining the confidentiality and authenticity of data, and can improve the security aspects of data or information. Cryptography is a field of science that studies data encoding techniques. Cryptography is divided into two types namely classic and modern, and has symmetrical and asymmetrical keys. On the symmetrical key there is an Advanced Encryption Standard (AES) or it can also be called Rijndael. AES is a secure chipper algorithm to protect data or information that is confidential by using encryption and decryption techniques with varying key lengths, namely 128bit, 192bit and 256bit. In 2001, AES was used as a standard cryptographic algorithm

Keywords*—Important data, cryptography, Advanced Encrypstion Standard (AES)*

Submitted: 20 September 2019, **Accepted:** 15 Oktober 2019, **Published:** November 2019
ISSN: 2685-4902 (online), Website: http://jurnal.umus.ac.id/index.php/intech

1. PENDAHULUAN

Keamanan dari suatu data merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan informasi terutama yang berisi informasi yang hanya boleh diketahui isinya oleh pihak yang berhak saja. Pengiriman data atau informasi tanpa dilakukan pengamanan akan beresiko terhadap penyadapan dan informasi yang ada di dalamnya dapat mudah diketahui oleh pihak-pihak yang tidak berhak. Salah satu hal penting dalam menjaga kerahasiaan dan keamanan data adalah dengan proses enkripsi. Pada kenyataannya ada banyak sekali tipe data yang dapat di-enkripsi, salah satu diantaranya adalah data teks. Saat ini sudah ada beberapa algoritma untuk menjaga keamanan data teks, seperti DES, VIGNERE, Blowfish. Masing-masing algoritma memiliki kelebihan yang berbeda-beda. Dalam penelitian ini penulis akan membahas mengenai algoritma AES untuk pengamanan data file teks. Dengan adanya implementasi algoritma AES pada file teks ini diharapkan dapat meningkatkan keamanan data yang di simpan dalam file teks melalui proses enkripsi dan deskripsi, sehingga orang yang tidak berhak tidak dapat mengakses atau membaca file tersebut.

Permasalahan yang terdapat pada desa Cipinang kecamatan Rajagaluh Kabupaten Majalengka adalah belum tersedianya sistem keamanan untuk mengamankan data. Sehingga peluang mengubah atau mengedit data penting oleh seseorang yang tidak berwenang presentasinya masih tergolong tinggi. termasuk data penyeleksian peserta JAMKESMAS. Selama ini perangkat desa hanya mengandalkan system *back up* data secara *mirroring* untuk data yang tersimpan pada media penyimpanan sehingga masih dapat dilihat keaslian dari data tersebut. Selain itu pihak yang tidak berwenang masih dapat mengubah berkas teks/dokumen penting yang tersimpan pada komputer. Adapun tujuan dari penelitian ini yaitu mengetahui konsep kriptografi untuk pengamanan data berbasis text dengan menggunakan algoritma AES. Algoritma AES dipilih karena kemampuannya dalam mengenkripsi dan mendekripsikan data dengan panjang kunci yang bervariasi yaitu 128 bit, 192 bit, dan 256 bit dan perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES [1].

Penelitian mengenai kriptografi AES pernah dilakukan oleh Sianturi (2013), menurutnya AES dapat mengamankan data inputan (plainteks) yang kemudian dienkripsi dengan menggunakan algoritma AES dapat menghasilkan enskripsi dan dekripsi secara lebih cepat [2]. Sedangkan pada penelitian lain mengemukakan bahwa algoritma AES dapat digunakan untuk mengenkripsi pesan teks kemudian disimpan menjadi sebuah file dokumen dan isi file dokumen tersebut dienkripsi lagi selanjutnya hasil enkripsi isi file dokumen tersebut dienkripsikan dan selanjutnya dikompresi dan disembunyikan pada sebuah file citra (gambar) agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian yang berlapis-lapis [3]. Selain itu algoritma AES pun pernah diimplementasikan pada sistem operasi android dan mikrokontroller arduino, dimana menurut hasil penelitiannya algoritma AES dapat meningkatkan dukungan terhadap aspek keamanan sistem kunci elektronik melalui sebuah handphone dan mikrokontroller arduino sebagai penerima kontrol. Setelah dilakukan pengujian, total waktu eksekusi maksimum sistem kunci elektronik kendaraan yang telah dibuat sebesar 385 ms pada jarak 20 m. Lama waktu tersebut masih lebih rendah dibanding batas kenyamanan pengguna yaitu di bawah 1000 ms sehingga sistem layak untuk diterapkan [4]. Implementasi algoritma AES juga pernah dilakukan untuk enkripsi dan dekripsi proses penyandian email, hasil penelitiannya menunjukkan bahwa keamanan dalam mengirimkan dan menerima email dapat lebih terjamin, walaupun pesan email dapat diambil oleh orang lain tetapi mereka tetap tidak akan bisa membacanya karena teks tampilan dalam bentuk karakter heksadesimal dan jika dijadikan string maka akan tampil sebagai simbol-simbol tidak jelas[5].

Penelitian ini menggunakan algoritma AES karena algoritma AES memiliki kecepatan komputasi enkripsi dan dekripsi, analisis statistik, dan perhitungan kesalahan. Selain itu algoritma AES juga bebas dalam serangan analisis statistik dengan menggunakan analisis histogram dan korelasi koefisien [6]

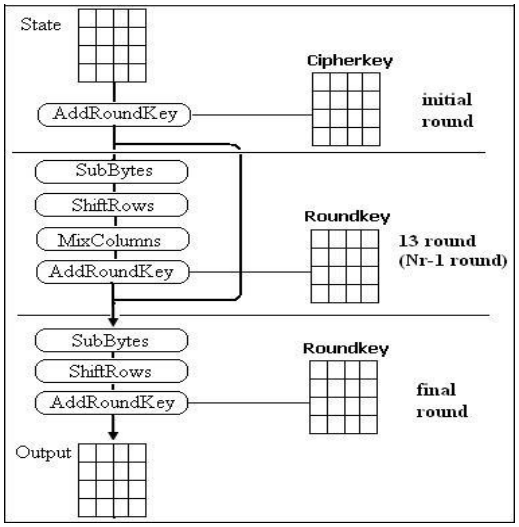
2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian terapan, dimana salah satu jenis penelitian yang bertujuan untuk memberikan solusi permasalahan tertentu secara praktis. Penelitian ini tidak berfokus pada pengembangan sebuah ide, teori, atau gagasan tapi lebih berfokus penerapan penelitian tersebut dalam kehidupan sehari-hari, dimana ciri utama dari penelitian ini adalah tingkat abstraksi yang rendah, dan manfaat atau dampaknya dapat dirasakan secara langsung [7].

Pemilihan metode AES didasarkan pada anggapan dasar bahwa AES adalah lanjutan dari algoritma enkripsi standar DES (*Data Encryption Standard*) yang masa berlakunya dianggap telah usai karena faktor keamanan, selain itu kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu kemanan, harga, dan karakteristik algoritma beserta implementasinya[8]. Berikut ini adalah operasi Rijndael (AES) yang menggunakan 128 bit kunci[9]:

1. Ekspansi kunci utama (dari 128 bit menjadi 1408 bit)
2. Pencampuran subkey
3. Diulang dari i=1 sampai i=10 Transformasi: *ByteSub* (subtitusi per *byte*) *ShiftRow* (Pergeseren byte per baris) *MixColumn* (Operasi perkalian GF(2) per kolom)
4. Pencampuran subkey (dengan XOR)
5. Transformasi : *ByteSub* dan *ShiftRow*

Adapun ilustrasi proses enskripsi AES dapat digambarkan seperti Gambar 1 [9]. Berdasarkan anggapan dasar tersebut, maka penulis dapat menyimpulkan hipotesis bahwa jika implementasi enkripsi dan dekripsi AES diterapkan maka keamanan data informasi peserta seleksi jamkesmas yang ada akan lebih maksimal dan lebih aman. Karena AES menggunakan kunci internal yang berbeda-beda, maka proses perputaran enkripsi dan dekripsi AES-128 akan dikerjakan sebanyak 10 kali, sedangkan pada proses enkripsi dan dekripsi AES-192 proses putaran akan dikerjakan 12 kali, dan untuk AES-256 proses putaran akan dikerjakan 14 kali[10].



Gambar 1. Proses enkripsi AES

Adapun kerangka berfikir pada penelitian ini terdapat pada Gambar 2. Berdasarkan gambar 2, penulis coba untuk menganalisis beberapa temuan yang di peroleh pada lokasi penelitian yaitu di Desa Cipinang Kecamatan Rajagaluh Kabupaten Majalengka. Setelah dilakukan studi pendahuluan melalui observasi dan wawancara dengan bagian arsip, serta manganalisis sumber data yang di peroleh pada lokasi penelitian, maka di temukan beberapa permasalahan yaitu:

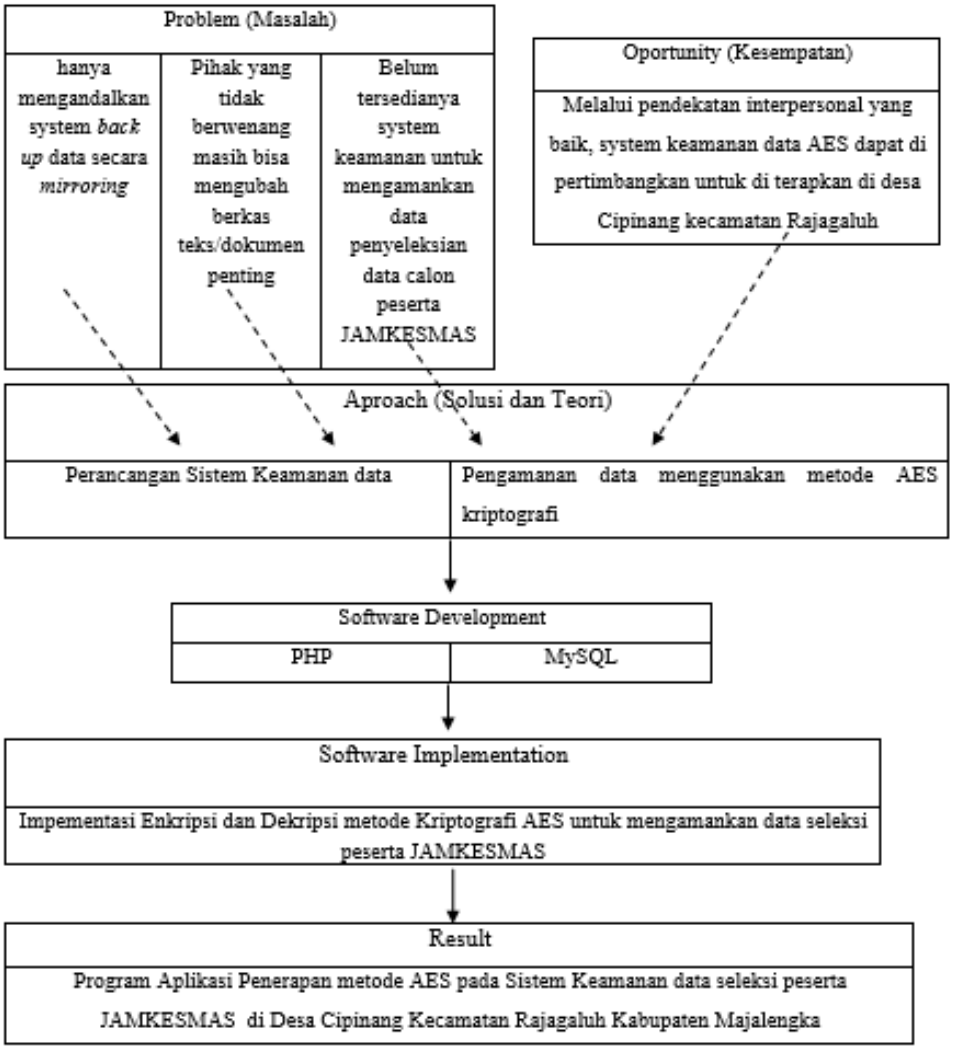
1. Permasalahan yang terdapat pada desa yaitu hanya mengandalkan system *Back up* data secara *mirroring*. Sehingga kesempatan atau peluang penyalahgunaan data atau edit data penting masih tergolong tinggi.

2. Permasalahan selanjutnya yaitu pihak yang berwenang masih bisa dengan bebas mengubah berkas teks / dokumen penting yang terdapat di desa.
3. Belum tersedianya system keamanan data untuk mengamankan data penyeleksian calon peserta JAMKESMAS.

Dari permasalahan yang ada, berarti Desa Cipinang Kecamatan Rajagaluh Kabupaten Majalengka membutuhkan sistem keamanan data yang dapat membantu mengamankan data - data penting yang terdapat di desa, contohnya yaitu data seleksi peserta JAMKESMAS. Untuk memecahkan permasalahan tersebut ditempuh langkah – langkah sebagai berikut:

1. Mengumpulkan data yang di perlukan untuk merancang serta membangun perangkat lunak yang nantinya akan di terapkan di Desa Cipinang Kecamatan Rajagaluh Kabupaten Majalengka.
2. Membuat aplikasi yang berupa system keamanan data yang digunakan untuk membantu bagian arsip untuk mengamankan data-data penting termasuk data seleksi peserta JAMKESMAS. Tools yang digunakan untuk membuat aplikasi yaitu menggunakan PHP disertai penggunaan database MySQL dan tools perancangan system yaitu *unified Modelling Language* (UML) dengan menggunakan usecase diagram, activity diagram dan class diagram.

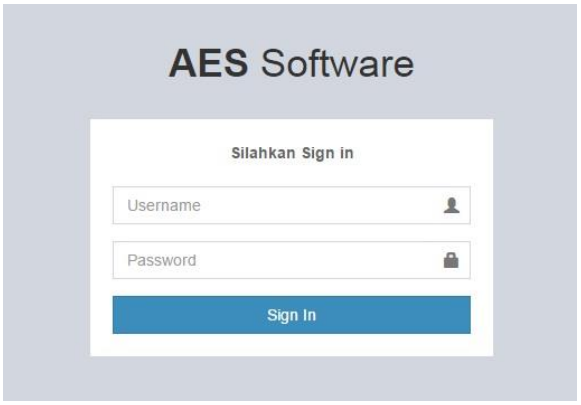
Diharapkan dengan dibuatnya system keamanan data ini dapat menyelesaikan permasalahan yang ada sehingga membantu pihak desa dalam mengamankan data-data penting contohnya yaitu data seleksi peserta JAMKESMAS.



Gambar 2. Kerangka berfikir penelitian

3. HASIL DAN PEMBAHASAN

Karna data yang ingin di enkripsi atau di dekripsi masih berbentuk *database*. Maka pertama yang dilakukan yaitu men-export dahulu data dari *database* yaitu dengan cara masuk terlebih dahulu ke dalam *PhpMyAdmin* lalu pilih *database* mana yang ingin di export. Selanjutnya untuk dapat melakukan enkripsi dan dekripsi data, admin/user harus masuk terlebih dahulu kedalam aplikasi AES dengan mengisikan *username* dan *password* yang telah tervalidasi. Implementasi login tersebut terdapat pada Gambar 3.



Gambar 3. Form login

a. Prosedur enkripsi AES

Langkah awal yaitu menentukan terlebih dahulu plaintext dan key nya. Tabel 1 dan Tabel 2 adalah plainteks dan key yang akan digunakan.

Tabel 1. *Plainteks* yang digunakan

V	E	R	G
A	M	A	N
A	C	A	K
E	P	0	1

Tabel 2. *Key* yang digunakan

A	R	I	F
W	A	H	Y
U	D	I	C
A	K	E	P

Setelah itu masukkan *Initial Round*. Untuk menghitung *initial round* ubah dahulu *plainteks* dan *key* menjadi bentuk biner, kemudian xor kan antara biner *plainteks* dan *key*. Hasil dari xor tersebut kemudian akan digunakan pada langkah selanjutnya yaitu untuk mencari *subbyte*. *Plainteks* hexa dan *key* hexa terdapat pada Tabel 3 dan 4.

Tabel 3. *Plainteks* hexa

56	45	52	47
41	4D	41	4E
41	43	41	4B
45	50	30	31

Tabel 4. *Key* hexa

41	52	49	46
57	41	48	59
55	44	49	43
41	4B	45	50

56 (Hexa) di ubah menjadi 1010110 (biner) sama hal nya dengan
41 (Hexa) di ubah menjadi 1000001 (biner). Lalu di Xor kan menjadi:

```
1010110
1000001   Xor
-------
0010111 = 17 (Hexa)
```

Langkah selanjutnya yaitu mencari subbyte untuk mendapatkan subbyte yaitu mensubsitusikan hasil dari XOR diatas dengan menggunakan tabel subbyte seperti Gambar 4.

	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. Tabel subbyte

Selanjutnya yaitu tahap *shiftrow*. Caranya yaitu table yang telah di *subbyte* diatas bagian baris pertama tidak ada yang berubah, baris kedua Bagian byte pertama di geser ke kiri. Lalu baris yang ketiga juga menggeserkan byte pertama dan kedua ke kiri. Dengan kata lain byte ke tiga dan byte ke 4 geser ke bagian byte awal dan byte kedua. Dan baris ketiga pun byte pertama, kedua dan ketiga pun geser ke kiri. Sehingga byte ke empat menempati byte pertama. Tabel 5 dan 6 merupakan shiftrow sebelum dan sesudah.

Tabel 5. Sebelum shiftrow

F0	F0	Af	7c
47	Fe	01	F0
Fa	C5	30	30
F2	Af	9d	ef

Tabel 6. Sesudah shiftrow

F0	F0	af	7c
fe	01	F0	47
30	30	fa	C5
ef	F2	af	9d

Selanjutnya yaitu Mix columns, dimana perhitungan mix columns akan mengkalikan satu kolom pertama byte dengan satu baris *matrix default*. Gambar 5 adalah contoh perhitungan mix columns.

F0	F0	Af	7c
Fe	01	F0	47
30	30	Fa	C5
Ef	F2	Af	9d

F0
fe
30
ef

02 03 01 01
01 02 03 01
01 01 02 03
03 01 01 02

Gambar 5. Perhitungan mix columns

Selanjutnya yaitu mencari *addroundkey*. Untuk mecari *addroundkey* xor-kan byte dari mixcolumns dengan *state keyschedule*. Gambar 6 adalah contoh perhitungan *addroundkey*.

3D Xor 8B =. b6

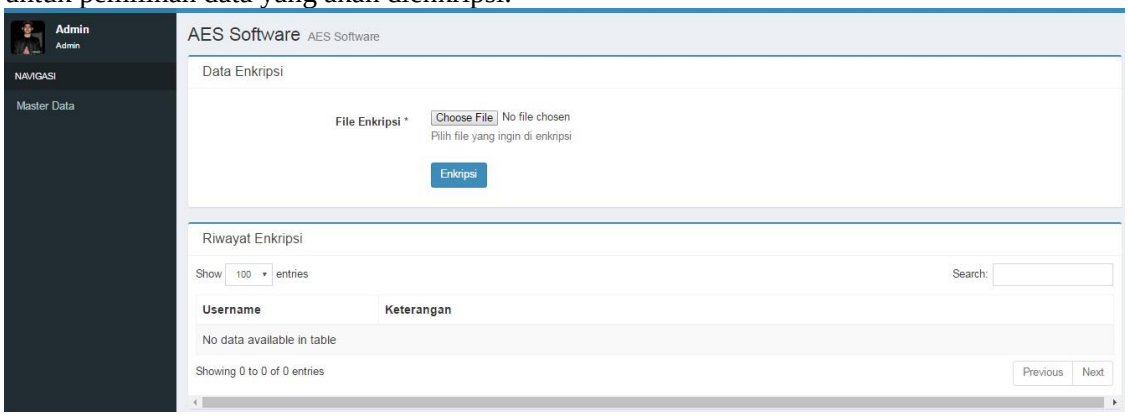
Gambar 6. Addroundkey

Ulangi sampai iterasi ke-10, namun pada saat iterasi ke 10, setelah melakukan step shift row tidak melakukan Mix Colum. Namun langsung melakukan XOR hasil state saat shift row dengan round key. Tabel 7 adalah chipertext yang terbentuk.

Tabel 7. chipertext

E5	A6	55	B3
Eb	83	Ba	81
C8	78	E0	9e
Bd	7c	Af	89

Implementasi untuk proses enkripsi ini terdapat pada Gambar 7. Choose file digunakan untuk pemilihan data yang akan dienkripsi.



Gambar 7. Form enkripsi data

b. Prosedur deskripsi AES

Langkah pertama dalam proses Dekripsi AES yaitu *inversAddrows* dimana Transformasi *InvAddRows* sama dengan transformasi *AddRows* yaitu menggunakan operasi XOR. Akan dilakukan proses XOR antara chipertext dengan kunci round yang digunakan pada saat enkripsi. Gambar 8 adalah xor antara chipertext dan key yang digunakan.

E5	A6	55	B3		Df	0d	6e	A9		3a	Ab	3b	1a
Eb	83	Ba	81		A0	A5	44	6a		4b	26	Fe	Eb
C8	78	E0	9e	XOR	15	21	64	45	=	Dd	59	84	Db
Bd	7c	Af	89		9b	52	95	9a		26	2e	3a	13

Gambar 8. Xor antara chipertext dan key

Selanjutnya yaitu *inversShiftrows* dimana Proses *inversShiftrows* adalah kebalikan dari proses *Shiftrows*. Dimana proses pergeseranya di mulai dari baris paling bawah. Gambar 9 adalah hasil pergeseran yang dilakukan.

3a	Ab	3b	1a
4b	26	Fe	Eb
Dd	59	84	Db
26	2e	3a	13

→

3a	Ab	3b	1a
Eb	4b	26	Fe
84	Db	Dd	59
2e	3a	13	26

Sebelum sesudah

Gambar 9. Hasil pergeseran

Langkah Langkah selanjutnya yaitu *InversSubbyte*. Pada Proses *InversSubbyte* sama dengan Proses *SubBytes*, namun tabel yang digunakan berbeda. Tabel yang digunakan adalah tabel inverse S-Box. Gambar 10 adalah hasil *InversSubbyte*

3a	Ab	3b	1a
Eb	4b	26	Fe
84	Db	Dd	59
2e	3a	13	26

→

A2	0e	49	43
3c	Cc	23	0c
4f	9f	C9	15
C3	A2	82	23

Gambar 10. Hasil *InversSubbyte*

Langkah selanjutnya yaitu *InversMixColomns*. Transformasi *InvMixColumns* sama dengan *MixColumns*, dimana perbedaanya adalah a(x) yang digunakan adalah inversnya(a-1). Gambar 11 adalah hasil transformasi *InvMixColumns*.

A2	0e	49	43
3c	Cc	23	0c
4f	9f	C9	15
C3	A2	82	23

xor

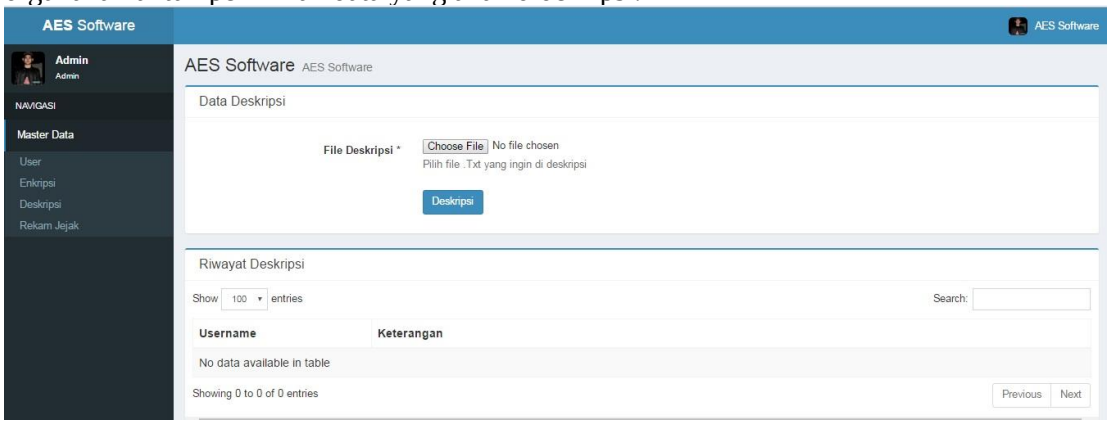
D8	D2	63	C7
5d	05	E1	2e
63	34	45	21
5d	C9	C7	0f

=

7a	dc	2a	84
61	C9	C2	22
2c	ab	8c	34
93	6b	45	2c

Gambar 11. Hasil transformasi *InvMixColumns*

Sedangkan implementasi untuk proses dekripsi ini terdapat pada Gambar 12. Choose file digunakan untuk pemilihan data yang akan didekripsi.



Gambar 12. Form dekripsi

Karena data seleksi peserta JAMKESMA ini termasuk kedalam data penting, maka peneliti menambahkan menu rekam jejak, yang digunakan untuk melihat rincian aktivitas user yang telah melakukan enkripsi maupun dekripsi data. Adapun prosedur rekam jejak adalah sebagai berikut:

1) Admin dapat melihat rincian berkas yang telah di enkripsi pada menu rekam jejak.
2) Lalu klik tombol "Rekam jejak" untuk melihat log aktivitas yang merekam aktivitas user dalam melakukan enkripsi dan dekripsi data admin maupun user.

Tampilan menu rekam jejak terdapat pada Gambar 13.

Gambar 13. Form rekam jejak

4. KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa keamanan data / dokumen hasil seleksi peserta JAMKESMAS dapat lebih maksimal karna data yang di simpan telah terenkripsi dan hanya bisa di lihat keaslian file tersebut apabila file tersebut telah di dekripsi. Selain itu file yang telah di enkripsi akan berubah ekstensi menjadi ".aes" dan file yang di dekripsi akan kembali menjadi ekstensi semula tanpa mengubah keaslian data tersebut.

5. SARAN

Setelah dilakukanya penelitian, maka saran yang di berikan adalah Aplikasi keamanan data AES belum bisa mendetekasi *keylogger* secara otomatis.

DAFTAR PUSTAKA

[1] Bhaudhayana, G.W., Widiartha, I.M., 2015, Implementasi Algoritma Kriptografi AES 256 dan Metode Stganografi LSB Pada Gambar Bitmap, *Jurnal Ilmiah Ilmu Komputer Universitas Udayana*, Vol.8 No.2 September, pp. 15-25, [online] Available : https://ojs.unud.ac.id/index.php/jik/article/view/18360/11888

[2] Sianturi, F.A., 2013, Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard, *Pelita Informatika Budi Darma*, Volume IV No.1, pp.42-46, [online] Available : https://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/208/208

[3] Pabokory, F.N., Astuti, I.F., Kridalaksana, A.H., 2015, Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard, *Jurnal Informatika Mulawarman*, Volume 10 No.1, pp.20-31, [online] Available : http://e-journals.unmul.ac.id/index.php/JIM/article/view/23/pdf

[4] Ramdhansya, A.F., Ariyanto, E., Nuha, H.H., 2014, Implementasi Advanced Encryption Standard (AES) Pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android dan Mikrokontroller Arduino, *Seminar Nasional Informatika UPN Veteran Yogyakarta*, 12 Agustus, pp.92-98, [online] Available : http://jurnal.upnyk.ac.id/index.php/semnasif/article/viewFile/1008/974

[5] Rosyadi, Ahmad., 2012, Implementasi Algoritma Kriptografi AES Untuk Enkripsi Dan Dekripsi Email, *Jurnal Transient*, Volume 1 No 3, pp.63-67, [online] Available : https://ejournal3.undip.ac.id/index.php/transient/article/view/19/1807

[6] Wahyu, M.A., 2018, Perbandingan Enkripsi Citra Digital Dengan Menggunakan Algoritma AES, RSA, dan Chaos, *Skripsi*, Program Studi Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta

[7] Guritno, Suryo., Sudaryono., Untung. Rahardja., 2011, *Theory and Application Of IT Research : Metodologi Penelitian Teknologi Informasi*, Andi : Yogyakarta

[8] Munawar., 2012, Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris, *Jurnal Komputer dan Informatika (KOMPUTA)*, Edisi I Volume I, pp.11-17, [online] Available : https://search.unikom.ac.id/index.php/komputa/article/view/51

[9] Sadikin, Rifki., 2010, *Kriptografi untuk Keamanan Jaringan dan Implementasinya Dalam Bahasa Java*, Andi : Yogyakarta

[10] Udayana, I.PA.E.D., Sastra, N.P., 2016, Perbandingan Performansi Pengamanan File Backup LPSE Menggunakan Algoritma DES dan AES, *Jurnal Teknologi Elektro*, volume 15 Nomor 01 Januari, pp.111-117, [online] Available : https://ojs.unud.ac.id/index.php/JTE/article/view/20966/14139