JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode *Advanced Encryption Standard* (AES)

Josua Syahputra Sianipar[1], Nurcahyo Budi Nuugroho[2], Ita Mariami[3]
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]josuasianipar264@gmail.com, [2]nurcahyobn@gmail.com, [3]itamariami66@gmail.com
Email Penulis Korespondensi: josuasianipar264@gmail.com

Abstrak
Kerahasiaan dari data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak. Data gaji adalah sebuah data yang dianggap sangat penting dan beresiko apabila terjadi penyalahgunaan dan manipulasi. Untuk itu dalam pencatatan data gaji karyawan PT. Alfa Scorpii Medan menggunakan file text dari Microsoft Excel, isi file akan diinput pada aplikasi yang digunakan, sehingga akan rawan terjadinya manipulasi dan penyalahgunaan data.Untuk mengatasi masalah tersebut dibutuhkan sebuah sistem yang mampu mengolah data menjadi tidak terbaca dengan teknik penyandian modern. Sehingga membantu pihak perusahaan dalam mengamankan data gaji karyawan, sehingga dapat dikelola dengan aman tanpa adanya kekhawatiran penyalahgunaan data oleh orang yang tidak bertanggung jawab. Teknik yang digunakan adalah ilmu kriptografi dengan algoritma AES. Advanced Encryption Standard merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandian blok (block cipher) yang memproses blok data 128-bit dengan panjang kunci 128-bit, 192-bit, dan 256-bit.Hasil penelitian merupakan terciptanya sebuah aplikasi kriptografi dengan metode AES 128 untuk mengamankan data gaji perusahaan.
Kata Kunci: Data Gaji, Alfa Scorpii, Kriptografi, AES 128

Abstract
Confidentiality of data or information is a complete service that is made to protect stored information from being read or opened by unauthorized parties. Salary data is data that is considered very important and is at risk in the event of misuse and manipulation. For this reason, in recording employee salary data at PT. Alfa Scorpii Medan uses a text file from Microsoft Excel, the contents of the file will be input into the application used, so it will be prone to data manipulation and misuse. Thus assisting the company in securing employee salary data, so that it can be managed safely without any worries of data misuse by irresponsible people. The technique used is cryptography with the AES algorithm. Advanced Encryption Standard is a symmetric cryptographic algorithm that operates in block cipher mode that processes 128-bit data blocks with 128-bit, 192-bit, and 256-bit key lengths. The result of this research is the creation of a cryptographic application using the AES method. 128 to secure company salary data.
Keywords*: Salary Data, Alfa Scorpii, Cryptography, AES 128*

1. PENDAHULUAN

Data merupakan komponen utama dari sistem informasi perusahaan. Kerahasiaan dari data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak. Upaya dalam menjaga kerahasiaan dari data atau informasi tersebut sudah tercetus sejak zaman dahulu tepatnya pada zaman Romawi dengan metode pergeseran huruf atau karakter dengan dasar nilai tertentu [1].

Dalam pencatatan data gaji karyawan PT. Alfa Scorpii Medan menggunakan *file text* dari *Microsoft Excel*, isi *file* akan diinput pada aplikasi yang digunakan, sehingga akan rawan terjadinya manipulasi dan penyalahgunaan data tersebut. Walaupun sebenarnya jika dianalisa menurut ISO 2700, tidak ada masalah terkait pemindahan aset fisik perusahaan. Yang berarti pengamanan harus dilakukan pada aset luar lokasi dengan mempertimbangkan risiko yang berada di luar lokasi. Namun demikian, tujuan dari kriptografi adalah untuk memastikan penggunaan kriptografi yang tepat dan efektif demi melindungi kerahasiaan, keaslian, dan atau integritas informasi [2].

Penelitian ini menjelaskan bagaimana pemanfaatan kriptografi dalam mengamankan data gaji karyawan. Kriptografi adalah metode untuk mencegah kebocoran data rahasia. Kriptografi memiliki dua proses utama yang terdiri dari proses enkripsi dan dekripsi. Proses enkripsi adalah proses pengkodean yang mengubah *plaintext* menjadi *ciphertext* menjadi teks-kode sehingga pesan sulit dimengerti. Dalam mengamankan data, kriptografi memiliki beberapa metode, salah satunya ialah metode *Advanced Encryption Standard* (AES).

Advanced Encryption Standard merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandian blok (*block cipher*) yang memproses blok data 128-bit dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Algoritma kriptografi pengganti DES ini dipublikasikan oleh NIST (*National Institute of Standards and Technology*) milik pemerintah Amerika Serikat pada 26 November 2001 [3].

Dari pembahasan penelitian tersebut diharapkan sistem pendataan gaji berbasis *desktop* ini, dapat membantu dan dapat dikelola dengan aman tanpa adanya kekhawatiran penyalahgunaan data oleh orang yang tidak bertanggung jawab.

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kata *cryptography* berasal dari Bahasa Yunani, yakni *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) sedangkan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Kata "seni" tersebut berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesannya. Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan [4]. Pengamanan pada data dilakukan untuk menjaga kerahasiaan informasi dan agar aman dari orang-orang yang tidak bertanggung jawab, maka dilakukanlah pengamanan data dengan menggunakan algoritma kriptografi [3].

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang akan dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari kata tersebut [5].

2.2 Advanced Encryption Standard

Advanced Encryption Standard didasarkan pada teknik enkripsi simetris. AES merupakan standar enkripsi lanjutan yang memberikan keamanan yang lebih baik daripada 3DES dan kekuatan keamanan jauh lebih baik daripada metode enkripsi lainnya. Ukuran kunci AES lebih kecil dibandingkan dengan skema yang lain. AES terdiri dari substitusi *byte* dan pergeseran baris dan ini membentuk transformasi lingkaran [7].

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde [8]. Jumlah ronde yang digunakan oleh AES terkait dengan panjang kunci yang dipakai seperti pada tabel 1 berikut ini.

Tabel 1. Hubungan Antara Jumlah Ronde dan Panjang Kunci AES

Panjang Kunci AES (bit)	Jumlah Ronde (Nr)
128	10
192	12
256	14

2.2.1 Proses Ekspansi Kunci

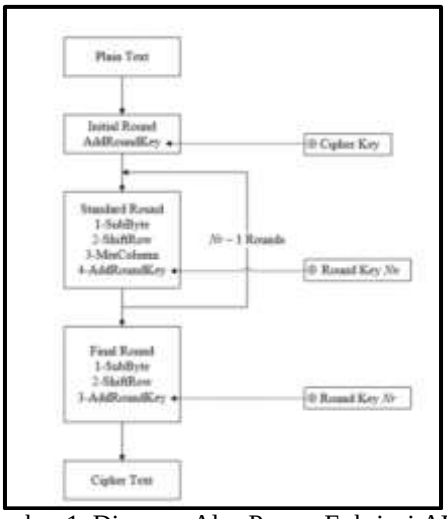
Proses ekspansi kunci dalam algoritma AES yang akan dipakai pada tiap tahap diperlukan dalam proses enkripsi. Untuk melakukan pengembangan jumlah kunci yang akan dipakai dari kunci utama maka dilakukan *key schedule*. Proses ini terdiri dari beberapa operasi, yaitu [10]:

1. Operasi *Rotate*, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
2. Operasi *SubBytes*, yaitu 8 bit dari *subkey* disubstitusikan dengan nilai dari *S-Box*.
3. Operasi *Rcon*, operasi ini akan diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari *user*.
4. Operasi XOR, dengan wi[-Nk] yaitu *word* yang berada pada Nk sebelumnya.

2.2.2 Struktur Enkripsi AES

Enkripsi adalah proses mengamankan informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Enkripsi di dalam AES menggunakan 4 jenis transformasi yaitu, *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*[8]. Pada awal proses enkripsi, blok-blok data masukan dan kunci dioperasikan dalam bentuk *array*. Setiap anggota *array* menghasilkan keluaran *ciphertext* yang dinamakan dengan *state*. Proses yang dilakukan setiap rondenya identik sama dari ronde ke-1 sampai dengan ronde ke Nr-1 (kecuali untuk ronde Nr). *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns* [12]. Untuk lebih jelasnya, struktur enkripsi AES dapat dilihat dari Gambar 1 berikut ini:

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi



Gambar 1. Diagram Alur Proses Enkripsi AES

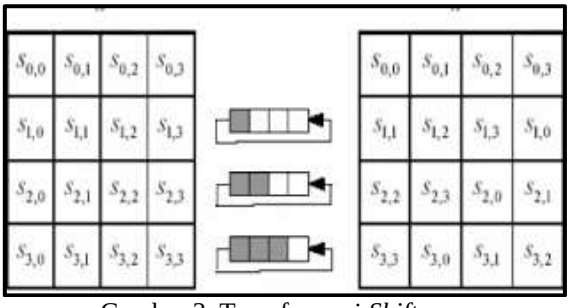
Garis besar algoritma AES yang beroperasi pada blok 128-bit dengan panjang kunci 128 bit adalah sebagai berikut:

1. *AddRoundKey*, dilakukan di awal dengan melakukan operasi XOR tiap *byte* pada plainteks dengan tiap *byte* pada *key*. Kemudian melakukan putaran sebanyak Nr-1 kali.
2. *SubBytes*, transformasi dimana setiap elemen akan dipetakan menggunakan sebuah tabel substitusi (S-Box). Tabel substitusi S-Box dapat dilihat di Gambar 2.

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

Gambar 2. Tabel Substitusi Untuk Transformasi *SubBytes*

3. *Shiftrows*, pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). Namun jumlah pergeseran yang dilakukan berbeda, tergantung untuk setiap barisnya. Baris pertama tidak terjadi pergeseran. Setiap *byte* dari baris kedua pada *plaintext* digeser satu *byte* ke kiri. Selanjutnya baris ketiga digeser ke kiri sebanyak dua *byte* dan pada baris keempat digeser ke kiri sebanyak tiga *byte*. Proses ini bertujuan untuk menghasilkan *diffusion* yakni dengan menyebarkan pengaruh transformasi nonlinear pada baris-baris plainteks untuk putaran selanjutnya. Transformasi *Shiftrows* dapat dilihat di Gambar 3.



Gambar 3. Transformasi *Shiftrows*

4. *MixColumns*, tiap kolom dari *plaintext* dilakukan operasi perkalian. Hal ini bertujuan untuk menyebarkan pengaruh setiap bit plainteks dan *key* terhadap cipherteks yang dihasilkan, pada arah kolom plainteks.

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

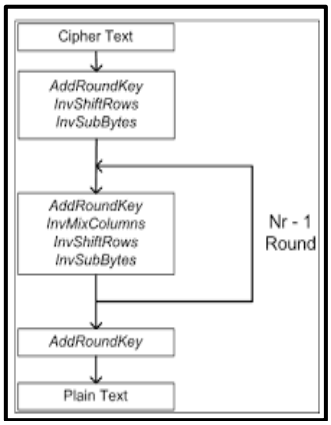
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

Gambar 4. Proses *MixColumns*

5. *AddRoundKey*, *key* yang telah ada diekspansikan terlebih dahulu, maka akan didapat *roundkey* yang akan digunakan untuk proses selanjutnya. Kemudian setiap *byte* dari plainteks keluaran proses *MixColumns* dilakukan operasi XOR dengan setiap *byte* dari *roundkey*. Semua proses enkripsi algoritma AES dilakukan hingga putaran ke-n dengan cara yang sama. Sedangkan untuk putaran terakhir proses *SubBytes*, *Shiftrows*, dan *AddRoundKey* tetap dilakukan tetapi proses *MixColumns* tidak dilakukan.

2.2.3 Struktur Dekripsi AES

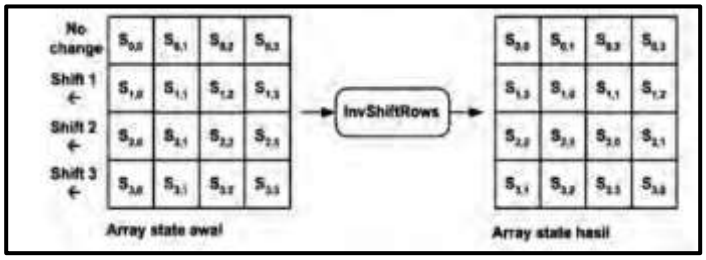
Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *inverse cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* [10]. Diagram alur proses dekripsi dapat dilihat pada Gambar 5.



Gambar 5. Diagram Alur Proses Dekripsi AES

Pada awal proses dekripsi, *input* yang telah disalin ke dalam *state* akan mengalami transformasi *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr.

a. *Inverse Shiftrows*, transformasi *byte* yang berkebalikan dengan transformasi *ShiftRows*. Pada transformasi ini, dilakukan pergeseran bit ke kanan sedangkan pada *ShiftRows* dilakukan pergeseran bit ke kiri. Ilustrasi transformasi ini terdapat pada gambar berikut.



Gambar 6. Transformasi *Inverse Shiftrows*

b. *Inverse SubBytes*, transformasi *bytes* yang berkebalikan dengan transformasi *SubBytes*. Pada proses ini, tiap elemen pada *state* dipetakan dengan menggunakan tabel *Inverse* S-Box.
c. *Inverse MixColumns*, Untuk melakukan dekripsi pesan, dilakukan *inverse* dari transformasi *MixColumns* yakni mengalikan setiap kolom dengan matriks perkalian dalam AES berikut :

$$\begin{bmatrix} 0B & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3. HASIL DAN PEMBAHASAN

3.1 Algoritma Sistem

Adapun algoritma yang akan digunakan dalam metode *Advanced Encryption Standard* adalah melakukan proses ekspansi kunci, proses enkripsi, dan proses dekripsi.

3.1.1 Proses Ekspansi Kunci

Kunci ronde (*round key*) dibutuhkan untuk proses enkripsi dan dekripsi pada algoritma *Advanced Encryption Standard*. Maksimal panjang kunci adalah 16 digit dan jumlah kunci rondenya adalah 10 kunci ronde yang diperoleh dari proses ekspansi kunci. Pada kasus ini, kunci yang akan digunakan yaitu "marhusorsianipar".

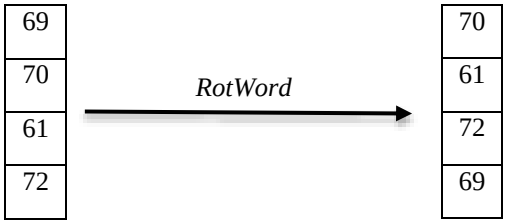
a. Urutkan kunci ke dalam blok berurutan 128 bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk heksadesimal.

m	a	r	h	u	s	o	r	s	i	a	n	i	p	A	r
6D	61	72	68	75	73	6F	72	73	69	61	6E	69	70	61	72

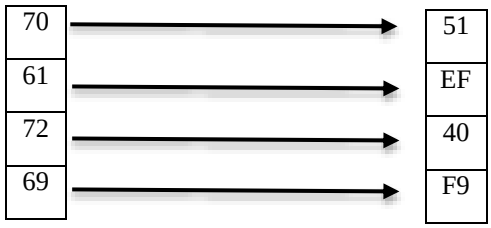
b. Langkah selanjutnya yaitu susun kunci yang telah diubah kedalam bentuk heksadesimal ke dalam *state* berukuran 4x4 seperti di bawah ini:

6D	75	73	69
61	73	69	70
72	6F	61	61
68	72	6E	72

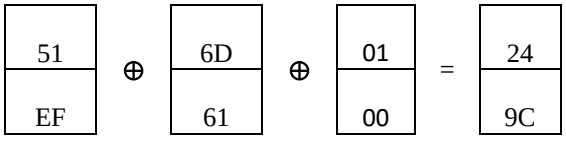
c. Setelah itu, untuk mendapatkan kolom pertama pada sub kunci, langkah pertama yaitu dilakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom ke-4 ke atas 1 kali dari kunci ronde ke-0.



d. Kemudian hasil dari *RotWord* tersebut disubstitusikan dengan nilai pada tabel S-Box (*SubBytes*).



e. Tahap yang terakhir yaitu lakukan proses XOR antara kolom pertama dari kunci ronde ke-0, hasil dari *SubBytes* lalu di-XOR-kan lagi dengan *Rcon*.



JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

40	72	00	2F
F9	68	00	8B

f. Untuk mendapatkan kolom kedua, diperoleh dari proses XOR antara *Wi* dengan kolom kedua dari kunci ronde ke-0. Sedangkan untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua

Kolom ke-2 Kolom ke-3 Kolom ke-4

24	⊕	75	=	51	51	⊕	73	=	22	22	⊕	69	=	4B
9C		73		EF	EF		69		86	86		70		F6
2F		6F		40	40		61		21	21		61		40
8B		72		F9	F9		6E		97	97		72		E5

g. Dari seluruh proses di atas, maka telah didapatlah ekspansi kunci untuk ronde ke-1 yaitu:

24	51	22	4B
9C	EF	86	F6
2F	40	21	40
8B	F9	97	E5

Untuk mendapatkan kunci ronde ke-2 sampai ke-10, proses di atas diulang 10 kali. Di bawah ini adalah hasil ekspansi kunci dari ronde ke-1 sampai ke-10:

24	51	22	4B
9C	EF	86	F6
2F	40	21	40
8B	F9	97	E5

Round Key ke-1

64	35	17	5C
95	7A	FD	0B
F6	B6	97	D7
38	C1	56	B3

Round Key ke-2 … *Round Key* ke-10

E3	FF	87	FF
05	E2	BB	20
15	C1	EE	49
F7	7C	49	55

3.1.2 Proses Enkripsi AES

Plaintext yang akan digunakan yaitu “FITRI NAINGGOLAN”. Kemudian urutkan ke dalam blok lalu ubah kedalam bilangan heksadesimal.

F	I	T	R	I		N	A	I	N	G	G	O	L	A	N
46	49	54	52	49	20	4E	41	49	4E	47	47	4F	4C	41	4E

Susun 16 *byte* pertama dari *plaintext* yang telah diubah ke dalam *state* 4x4:

46	49	49	4F
49	20	4E	4C
54	4E	47	41
52	41	47	4E

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Lakukan XOR antara *plaintext* dengan *RoundKey* 0. Proses ini dinamakan *AddRoundKey*.

46	49	49	4F	⊕	6D	75	73	69	=	2B	3C	3A	26
49	20	4E	4C		61	73	69	70		28	53	27	3C
54	4E	47	41		72	6F	61	61		26	21	26	20
52	41	47	4E		68	72	6E	72		3A	33	29	3C

Proses *AddRoundKey* di atas masih sebagai *pra-round* dan akan menjadi masukan untuk ronde ke-1 yang akan diproses dengan 4 transformasi yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*.

Round 1

Text

2B	3C	3A	26
28	53	27	3C
26	21	26	20
3A	33	29	3C

SubBytes

F1	EB	80	F7
34	ED	CC	EB
F7	FD	F7	B7
80	C3	A5	EB

Shiftrows

F1	EB	80	F7
ED	CC	EB	34
F7	B7	F7	FD
EB	80	C3	A5

MixColumns

CB	B5	09	F1
D9	6A	8C	26
CF	C9	C0	D6
D7	46	1A	9A

RoundKey 1

24	51	22	4B
9C	EF	86	F6
2F	40	21	40
8B	F9	97	E5

AddRoundKey

EF	E4	2B	BA
45	85	0A	D0
E0	89	E1	96
5C	BF	8D	7F

Lakukan proses di atas sampai 10 kali putaran (round). Berikut ini adalah hasil enkripsi hinga *round* ke-10:

Round ke-1

EF	E4	2B	BA
45	85	0A	D0
E0	89	E1	96
5C	BF	8D	7F

Round ke-2

AF	80	1E	AD
4C	10	71	2D
39	7F	57	01
EF	87	4C	29

Round ke-3

80	CA	61	C5
42	8B	90	31
54	E4	7A	BB
A5	F5	FF	CC

Round ke-4

78	79	AD	61
7E	2C	D6	6B
E5	CE	7D	06
BD	9F	26	F0

Round ke-5

75	C7	DF	B7
79	8C	30	D4
27	A6	12	D4
27	6F	0F	E5

Round ke-6

F4	F8	92	2C
0E	5B	01	5A
75	1C	C7	D3
7D	C5	8C	73

Round ke-7

A4	97	B0	95
65	E7	8C	5A
6B	B8	B6	A5
BC	AE	64	0D

Round ke-8

34	68	6D	F1
EA	D4	32	E4
E3	94	EB	8E
FF	86	A4	B3

Round ke-9

0A	A9	71	89
80	8D	D5	BD
46	1D	3F	71
9C	CD	2F	86

Round ke-10

D5	84	8A	8F
C1	A8	A7	CE
62	C2	A7	88
B0	E5	AA	E4

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3.1.3 Proses Dekripsi AES

Kunci yang digunakan untuk proses dekripsi sama dengan yang digunakan pada proses enkripsi. Berikut adalah proses dekripsi dari hasil *ciphertext* yang telah diperoleh dari proses enkripsi sebelumnya.

Gn	R2	AI	NA	Ix	Dd	p7	yU	/3	xJ	T3	DD	9w	Wn	iA	Pt
D5	84	8A	8F	C1	A8	A7	CE	62	C2	A7	88	B0	E5	AA	E4

Round 1

Ciphertext

D5	84	8A	8F
C1	A8	A7	CE
62	C2	A7	88
B0	E5	AA	E4

Text

D5	84	8A	8F
C1	A8	A7	CE
62	C2	A7	88
B0	E5	AA	E4

RoundKey 10

E3	FF	87	FF
05	E2	BB	20
15	C1	EE	49
F7	7C	49	55

Initial Round

36	7B	0D	70
C4	4A	1C	EE
77	03	49	C1
47	9F	E3	93

InvShiftRows

36	7B	0D	70
EE	C4	4A	1C
49	C1	77	03
E3	93	47	9F

InvSubBytes

24	03	F3	D0
88	5C	C4	99
02	D5	A4	DD
16	6E	4D	22

RoundKey 9

C1	1C	78	78
59	E7	59	9B
89	D4	FF	A7
4B	8B	35	1C

AddInvRoundKey

E5	C2	8B	A8
D1	BB	9D	02
8B	5C	5B	7A
5D	E5	78	3E

InvMixColumns

95	28	33	84
81	02	7B	2F
CC	5E	87	43
3F	E6	55	7E

Round 10

Text

2E	72	4E	03
93	16	61	5D
3E	8B	86	93
D4	D4	9B	10

InvShiftRows

2E	72	4E	03
5D	61	16	93
86	93	3E	8B
D4	9B	10	D4

InvSubBytes

C3	1E	B6	D5
8D	D8	FF	22
DC	22	D1	CE
19	E8	7C	19

RoundKey 0

6D	75	73	69
61	73	69	70
72	6F	61	61
68	72	6E	72

AddInvRoundKey

46	49	73	4F
49	20	4E	4C
54	4E	47	41
52	41	47	4E

Hasil dari proses *AddRoundKey* atau *round* ke-10 ubah ke bentuk karakter di dalam tabel ASCII.

Round	**Kode ASCII**	**Karakter**
46	70	F
49	73	I
54	84	T
52	82	R
49	73	I

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

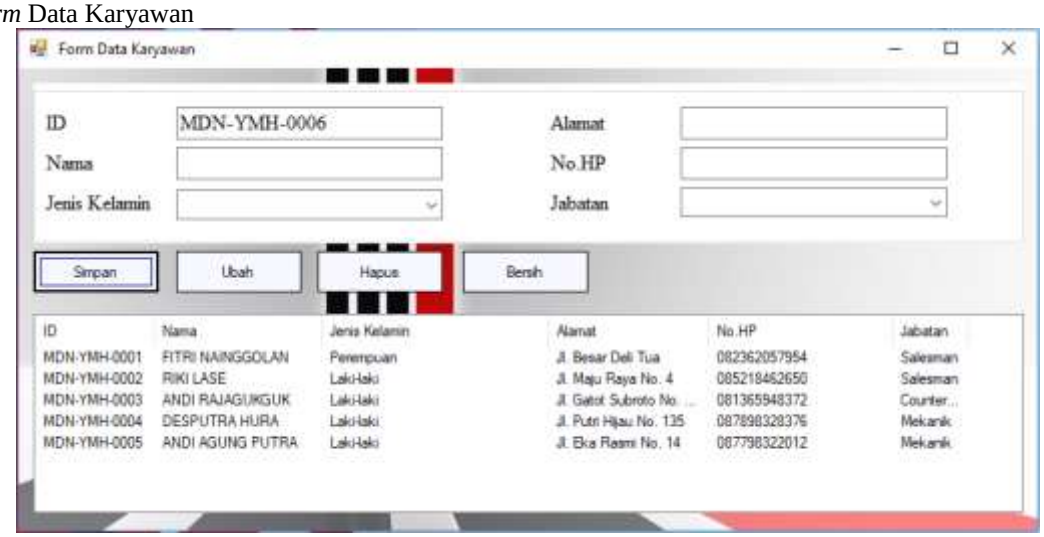
20	32	Spasi
4E	78	N
41	65	A
49	73	I
4E	78	N
47	71	G
47	71	G
4F	79	O
4C	76	L
41	65	A
4E	78	N

3.2 Implementasi Sistem

1. *Form* Menu Utama

Gambar 7. Tampilan *Form* Menu Utama

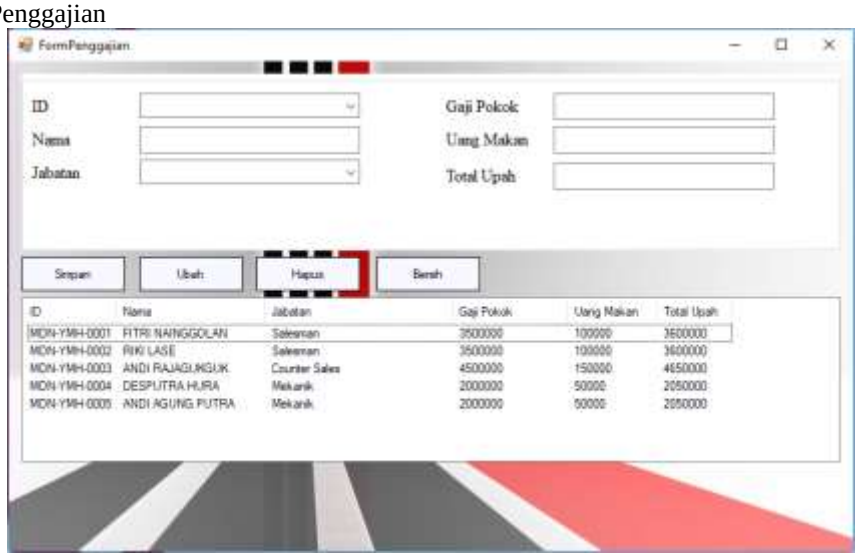
2. *Form* Data Karyawan



Gambar 8. Tampilan *Form* Data Karyawan

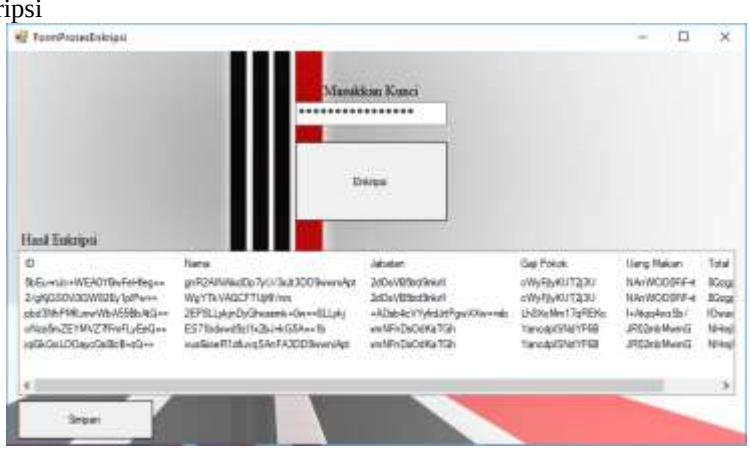
JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3. *Form* Data Penggajian



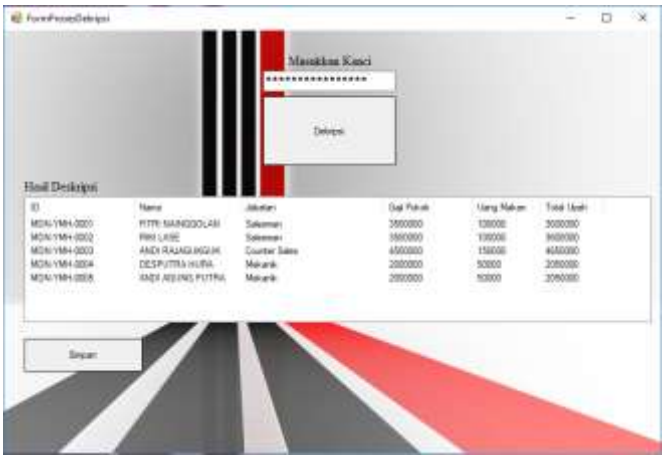
Gambar 9. Tampilan *Form* Data Penggajian

4. *Form* Proses Enkripsi



Gambar 10. Tampilan *Form* Proses Enkripsi

5. *Form* Dekripsi



Gambar 11. Tampilan *Form* Proses Dekripsi

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 1, Januari 2024, Hal 35-45
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

4. KESIMPULAN

Berdasarkan pembahasan dalam pengamanan data gaji karyawan dengan menggunakan metode *Advanced Encryption Standard* terhadap sistem yang dirancang dan dibangun maka dapat ditarik kesimpulan bahwa algoritma AES mampu untuk mengamankan data gaji karyawan.

Dalam mengujikan pengamanan data gaji karyawan pada PT. Alfa Scorpii-Sentral Yamaha Medan, dimulai dari memasukkan data karyawan kemudian melakukan proses enkripsi dilanjutkan dengan proses dekripsi dan membandingkan dengan hasil enkripsi dengan dekripsi melihat sejauh mana apikasi dapat mengembalikan data semula.

UCAPAN TERIMAKASIH

Terima kasih diucapkan kepada kedua orang tua serta keluarga yang selalu memberi motivasi, doa, dan dukungan moral maupun materi serta pihak-pihak yang telah mendukung dalam proses pembuatan jurnal ini yang tidak dapat disebutkan satu per satu. Kiranya jurnal ini bias memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

DAFTAR PUSTAKA

[1] Astri Prameshwari, Nyoman Putra Sastra, "Implementasi Algoritma *Advanced Encryption Standard* (AES) 128 Untuk Enkripsi dan Dekripsi *File* Dokumen", Eksplora Informatika, Vol. 8, No. 2, 2018, pp.52-58.
[2] IT Governance Indonesia, DATA GAJI PEKERJA FACEBOOK BOCOR, Bagaimana Cara Mencegahnya? Berdasarkan ISO 27000, ITG.ID, Des.2019.[Online].Available: https://itgid.org/fb [Akses : 14 Jul. 2021].
[3] Jaka Prayudha, Saniman, Ishak, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode *Advanced Encryption Standard* (AES), Sains dan Komputer (SAINTIKOM), Vol. 18, No.2, Agustus 2019, pp.119-129.
[4] Ashari Arief, Ragil Saputra, "Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi *Instant Messaging*", Scientific Journal of Informatics, Vol. 3, No.1, Mei 2016, pp.46-54.
[5] Freshly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*", Jurnal Informatika Mulawarman, Vol. 10, No.1, Feb.2015, pp.20-31.
[6] Budi Hartono, "Ruang Lingkup Kriptografi Untuk Mengamankan Data", Vol. 9, No.2, Mei 2004, pp.1-2.
[7] Putu Warna Putra, Made Sudarma, Nyoman Pramaita, "Rancang Bangun Sistem Enkripsi Dan Dekripsi SMS Menggunakan AES dan *Blowfish Cipher* serta Kombinasinya Pada Telepon Seluler Berbasis Android", Majalah Ilmiah Teknologi Elektro, Vol. 18, No. 1, Jan.2019, pp.1-8.
[8] Aditia Rahmat Tulloh, Yurika Permanasari, Erwin Harahap, "Kriptografi *Adcvanced Encryption* (AES) Untuk Penyandian File Dokumen", Jurnal Matematika UNISBA, Vol. 15, No. 1, Mei 2016, pp.1-8.
[9] Ratno Prasetyo, Asep Suryana, "Aplikasi Pengamanan Data dengan Teknik Algoritma Kriptografi AES dan Fungsi Hash SHA-1 Berbasis Desktop", Jurnal SISOKOM, Vol. 5, No.1, Sept.2016, pp.61-65.
[10] Faturungi Muharram, Huzain Azis, Abdul Rachman Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)", Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi, Vol. 3, No. 2, Des.2018, pp.112-115.