Jurnal CyberTech

Vol.1. No.10, Desember 2018, pp. xx~xx
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Kriptografi Untuk Pengamanan Data Gaji Staff Pada Klinik Pratama Siti Rahmah Menggunakan Metode *Advanced Encryption Standard* (AES)

Nabilah Qomariah [1], Azanuddin [2], Vina Winda Sari[3]

[1,3] Program Studi Sistem Informasi, STMIK Triguna Dharma
[2] Program Studi Sistem Komputer, STMIK Triguna Dharma

Article Info

Article history:

Keyword:
Kriptografi
Data Gaji
Advanced Encryption Standard

ABSTRACT

Gaji merupakan pembayaran atas tenaga atau jasa yang di berikan kepada karyawan. Pemberian gaji merupakan masalah yang sangat penting karena mempunyai pengaruh yang sangat besar terhadap semangat kerja para karyawannya. Data gaji merupakan data yang bersifat rahasia dimana data ini hanya dapat di lihat oleh pihak tertentu seperti bagian keuangan atau kepala kantor. Klinik Pratama Siti Rahmah berusaha untuk mengamankan data tersebut agar terhindar dari penyalahgunaan atau manipulasi data oleh oknum yang tidak bertanggung jawab yang dapat mengakibatkan kerugian pada pihak klinik.Oleh karena itu diperlukan adanya sistem pengamanan yang dapat melakukan penyandian terhadap data. Pengamanan dilakukan dengan menggunakan algoritma kriptografi. algoritma yang digunakan adalah algoritma Advanced Encryption Standard 128 bit (AES).

Corresponding Author:
Nama : Nabilah Qomariah Dolok Saribu
Program Studi : Sistem Informasi
STMIK Triguna Dharma
Email : qomariahnabilah2804@gmail.com

1. PENDAHULUAN

Perkembangan teknologi dan informasi pada saat ini berkembang dengan pesat sehingga media ini banyak digunakan hampir diseluruh dunia. Dengan perkembangan teknologi informasi maka berkembang pula tindak penyalahgunaan terhadap informasi. Ada dua jenis informasi yaitu informasi yang bersifat umum yakni informasi yang boleh dilihat atau atau dibaca oleh siapa saja dan ada informasi yang bersifat rahasia dimana informasi ini hanya boleh dilihat atau dibaca oleh pihak-pihak tertentu[1]. Oleh karena itu diperlukan keamanan data yang baik untuk mengamankan informasi.

Ada begitu banyak data atau informasi yang perlu diamankan salah satunya adalah data gaji. Data gaji merupakan data yang bersifat rahasia dimana data ini hanya dapat di lihat oleh pihak tertentu seperti bagian keuangan atau kepala kantor. Adapun kasus penyalahgunaan data gaji disalah satu puskesmas di Medan, Penggajian pada puskesmas ini dilakukan dengan cara mentransfer ke rekening masing-masing staff, namun pada proses pengecekan di rekening salah satu staff tidak terjadi penambahan saldo dalam rekening tersebut, sehingga staff tersebut melaporkan ke pihak keuangan namun pihak keuangan puskesmas dapat menunjukkan bukti pengiriman. Hal ini terjadinya karena kurangnya pengamanan pada data gaji sehingga oknum yang tidak bertanggung jawab dapat menyalahgunakan atau memanipulasi data gaji yang menyebabkan kerugian

pada pihak puskesmas. Oleh karena itu, klinik Pratama Siti Rahmah yang bergerak di bidang kesehatan di wilayah kota Medan dengan jumlah karyawan mencapai puluhan orang berusaha untuk mengamankan data gaji agar hal yang sama tidak terjadi pada klinik tersebut. Data gaji pada klinik ini yaitu *file text* dari *Microsoft Exel* , isi *file* ini akan di *input* pada aplikasi yang digunakan, proses ini akan rawan terjadinya penyalahgunaan dan manipulasi data yang akan menyebabkan kerugian pada Klinik. Dalam hal ini dibutuhkan aplikasi keamanan untuk mengamankan data gaji dengan menggunakan kriptografi.

Kriptografi merupakan metode keamanan data yang mempunyai dua proses yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah data asli (*plaintext)* menjadi data yang tidak biasa atau sulit dipahami (*chipertext).* Sedangkan dekripsi merupakan kebalikannya, yaitu mengubah kembali data yang telah dienkripsi menjadi data asli yang bisa dibaca. Dalam kriptografi terdapat banyak algoritma penyadian data salah satunya adalah algoritma *Advanced Encryption Standart* (AES)[2].

Algoritma *Advanced Encryption Standart* (AES) adalah algoritma kriptografi simetrik yang beroperasi dalam penyadian blok (*block cipher)* yang memproses blok data 128-bit dengan panjang kunci 128-bit, 196-bit dan 256-bit. Penyadian AES menggunakan proses yang berulang disebut dengan ronde. Jumlah ronde tergantung panjang kunci yang digunakan. Enkripsi pesan teks pada AES adalah trasformasi terhadap state secara berulang dalam beberapa ronde[3].

2. METODE PENELITIAN

Metode penelitian adalah langkah-langkah yang dilakuakan peneliti untuk mendapatkan data atau informasi yang valid. Metode penelitian menggambarkan rancangan penelitian antara lain prosedur,langkah yang harus ditempuh, waktu penelitian, sumber data, proses pengambilan data, Proses pengolahan data dan selanjutnya proses analisis data. Berikut beberapa langkah-langkah yang dilakukan dalam penelitian ini yaitu:

2.1 Teknik Pengumpulan Data

Teknik yang digunakan dalam proses pengumpulan data sebagai berikut:

1. Observasi
   Observasi dalam penelitian dilakukan dengan tinjauan langsung ke klinik Pratama Siti Rahmah. Di klinik tersebut dilakukan analisis masalah yang dihadapi selama ini terkait keamanan data gaji.
2. Wawancara
   Setelah melakukan observasi, peneliti melakukan wawancara kepada bagian keuangan atau pihak yang bertanggung jawab dalam proses pengolahan data gaji diklinik Pratama Siti Rahmah.

Berikut ini adalah data penelitian berupa data staff dan data gaji yang didapatkan dari klinik Pratama Siti Rahmah yang akan digunakan dalam penelitian ini

Tabel 2.1 Data Staff Klinik Siti Rahamhah

No	NIK	NAMA	Tanggal Lahir	Alamat	Jabatan	Jenis Kelamin	No_Telp
1.	1209311504830001	TANTI WINDA ASTARI	27/05/1988	Gg. Rahayu	Analis	Perempuan	085398657743
2.	1209312501640002	dr. DIRA SARI PUJI	25/01/1964	Tirta Deli	Dokter Jaga	Perempuan	081267881039
3.	1209310705760002	INTAN NELA PERMATA	07/05/1976	Batang Kuis	Bidan	Perempuan	081326778904
4.	1209310102960001	TINA WIRANTI	01/021/996	Jl. Industri	Perawat	Perempuan	087798334561
5.	1209312804940002	HANNY SORAYA	28/04/1994	Naga Rejo	Administrasi	Perempuan	085967554321

Tabel 2.2 Data Gaji Staff Klinik Siti Rahmah

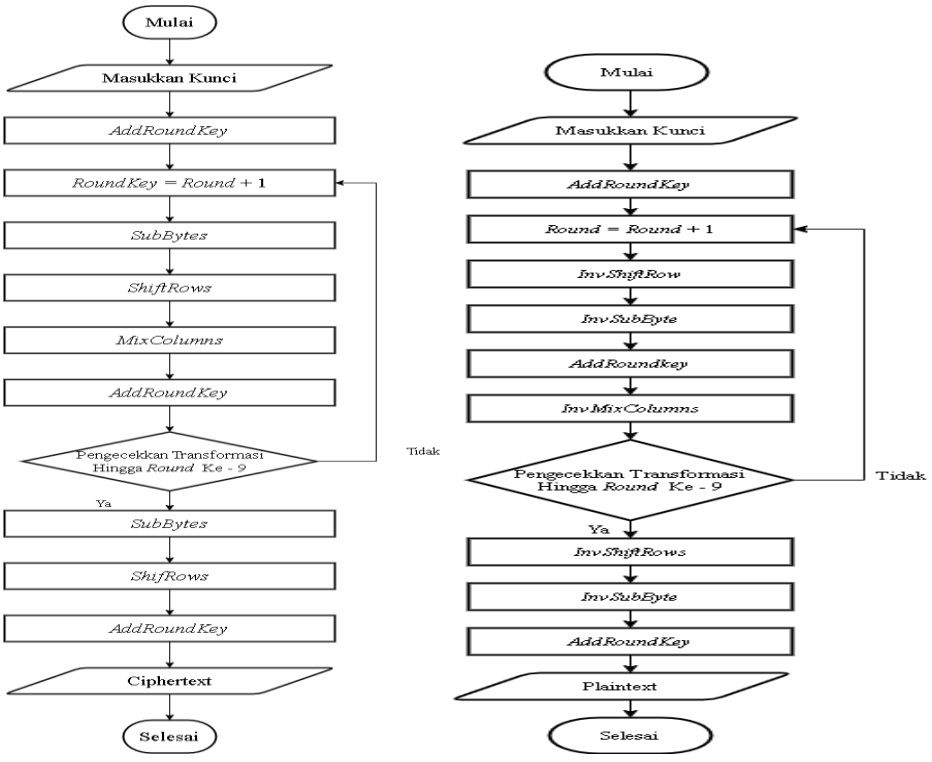
No	NIK	Nama Staff	Jabatan	Gaji Pokok	Tunjangan	Lembur	Uang Makan	Transpo-rtasi	Bonus
1.	1209311504830001	TANTI WINDA ASTARI	Analis	Rp.2200000	Rp.100000	Rp.100000	Rp.200000	Rp.100000	Rp.50000
2.	1209312501640002	dr. DIRA SARI PUJI	Dokter Jaga	Rp.6000000	Rp.500000	0	Rp.300000	Rp.100000	Rp.100000
3.	12093105760002	INTAN NELA PERMATA	Bidan	Rp.2500000	Rp.100000	Rp.50000	Rp.200000	Rp.100000	Rp.80000
4.	1209310102960001	TINA WIRANTI	Perawat	Rp.2200000	Rp.100000	Rp.120000	Rp.200000	Rp.100000	Rp.50000
5.	1209312804940002	HANNY SORAYA	Admini strasi	Rp.2200000	Rp.100000	Rp.100000	Rp.200000	Rp.100000	Rp.50000

2.2 *Flowchart* Metode *Advanced Encryption Standard* 128*bit*

Flowchart adalah sebuah metode penggambaran alur logika yang diterapkan pada sebuah algoritma untuk membagi masalah kedalam bagian-bagian yang lebih kecil dan mempermudah dalam menganalisis alternatif-alternatif lain dalam pengoperasian[4]. Dalam metode AES 128 bit langkah yang pertama yang dilakukan untuk mengamankan data gaji adalah mencari ekspansi kunci. Kunci ini digunakan disetiap ronde transformasi pada AES. Berikut langkah-langkah yang terdapat dalam proses ekspansi kunci:

1. AddroundKey, pada proses ini *plaintext* akan di XOR-kan dengan *Roundkey* ke-0.
2. Putaran, proses yang dilakukan pada setiap putaran adalah:
   a. RotWord, yaitu mengambil kata [a0, a1, a2, a3] sebagai masukkan dan melakukan perputaran permutasi menjadi [a1, a2, a,3, a0].
   b. SubByte, mensubtitusikan hasil dari RotWord dengan tabel S-Box.
   c. Rcon, pada kolom pertama dari *Roundkey* ke-0 dan hasil dari SubByte akan XOR-kan dengan Rcon[5].

Berikut ini adalah *flowchart* enkripsi dan dekripsi dari *Advanced Encryption Standart* (AES) :



Gambar 2.1 *Flowchart* enkripsi dan dekripsi *advanced encryption standard* 128*bit.*

2.3 Penyelesaian Masalah dengan Metode *Advanced Encryption Standard* 128*bit*

Berikut ini adalah penyelesaian masalah mengenai pengamanan data gaji Klinik Pratama Siti Rahmah dengan metode *Advanced Encryption Standard* 128bit :

1.3.1 Ekspansi Kunci

Ekspansi kunci dibutuhkan untuk proses enkripsi dan deskripsi pada tahapan *AddRoundKey*. Maksimal panjang kunci *pada Advanced Encryption Standard* 128 bit adalah 16 digit yang membutuhkan 10 kunci ronde. Kunci yang digunakan pada kasus ini adalah "KLINIKSITIRAHMAH". Berikut adalah proses ekspansi kunci *advanced encryption standard* 128 bit:

3. Urutkan *plaintext* kunci kedalam blok berukuran 128 bit (16 Kode ASCII), kemudian kunci diubah kedalam bentuk *Hexadecimal.*

K	L	I	N	I	K	S	I	T	I	R	A	H	M	A	H
4B	4C	49	4E	49	4B	53	49	54	49	52	41	48	4D	41	48

2. Selanjutnya adalah mengubah kunci yang telah diubah ke dalam *state* 4 x 4 seperti berikut:

4B	4C	49	4E
49	4B	53	49
54	49	52	41
48	4D	41	48

→ *RoundKey* ke-0

3. Setelah itu, melakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom 4 ke atas 1 kali menggunakan *RoundKey* ke-0 untuk menghasilkan *RoundKey* ke-1.

4E	→	49
49		41
41		48
48		4E

4. Selanjutnya, melakukan substitusi hasil dari *RotWord* dengan nilai yang ada pada tabel S-Box Rijndael (*SubBytes*).

49	→	3B
41	→	83
48	→	52
4E	→	2F

5. Selanjutnya, untuk mendapatkan kolom pertama dari *RoundKey* ke-1 adalah proses XOR antara kolom pertama dari *RoundKey* ke-0 dan hasil dari *SubBytes* di XOR-kan dengan *Rcon (Round Constanta)*.

4B	⊕	3B	⊕	01	=	71	Kolom ke-1
49		83		00		CA	
54		52		00		06	
48		2F		00		67	

6. Untuk mendapatkan nilai kolom selanjutnya dilakukan XOR antara kolom pertama (Wi) dengan kolom kedua dari *RoundKey* ke-0, kemudian untuk mendapatkan kolom berikutnya lakukan proses seperti kolom kedua.

4C	⊕	71	=	3D	Kolom ke-2
4B		CA		81	
49		06		4F	
4D		67		2A	

49	⊕	3D	=	74	Kolom ke-3
53		81		D2	
52		4F		1D	
41		2A		6B	

4E		74		3A	Kolom ke-4
49	⊕	D2	=	9B	
41		1D		5C	
48		68		23	

7. Dari seluruh proses yang telah dilakukan seperti di atas, maka didapatlah *RoundKey* ke-1, yaitu :

71	3D	74	3A
CA	81	D2	9B
06	4F	1D	5C
67	2A	6B	23

Untuk mendapatkan *RoundKey* ke-2 sampai dengan *RoundKey* ke-10, proses di atas diulang sebanyak 10 kali. Di bawah ini merupakan hasil ekspansi kunci dari setiap *round* yang akan digunakan untuk proses enkripsi dan dekripsi:

RoundKey ke-1

71	3D	74	3A
CA	81	D2	9B
06	4F	1D	5C
67	2A	6B	23

RoundKey ke-2

67	5A	2E	14
80	01	D3	48
20	6F	72	2E
E7	CD	A6	85

….

RoundKey ke-10

39	86	71	0D
7D	73	A6	D0
B8	71	E2	F9
21	1E	1E	A9

1.3.2 Enkripsi

Proses enkripsi algoritma AES mencakup 4 jenis transformasi *bytes*, yaitu *SubByte*, *ShiftRow*, *MixColumns* dan *AddRoundKey*[6]. Proses enkripsi akan dilakukan pada *record database* data gaji pada Klinik Pratama Siti Rahmah. *Plaintext* yang dienkripsi adalah "TANTIWINDAASTARI", dengan proses enkripsi seperti berikut ini:

1. *Plaintext* diurutkan kedalam blok dan diubah kedalam bentuk bilangan *hexadecimal*.

T	A	N	T	I	W	I	N	D	A	A	S	T	A	R	I
54	41	4E	54	49	57	49	4E	44	41	41	53	54	41	52	49

2. *Plaintext* disusun kedalam *state* 4 x 4.

54	41	4E	54
49	57	49	4E
44	41	41	53
54	41	52	49

3. Selanjutnya proses *AddRoundKey*, pada proses ini XOR-kan *plaintext* dengan *RoundKey* ke-0.

54	41	4E	54		4B	4C	49	4E		1F	0D	07	1A
49	57	49	4E		49	4B	53	49		00	1C	1A	07
44	41	41	53	⊕	54	49	52	41	=	10	08	13	12
54	41	52	49		49	4D	41	48		1C	0C	13	01

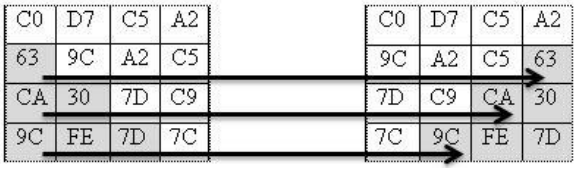
4. Hasil dari *AddRoundKey* diatas akan menjadi *round* ke-1 untuk diproses dengan 4 transformasi, yaitu *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey*.
   a. Transformasi pertama yaitu *SubBytes*, pada tahap ini setiap *byte* akan ditukar dengan tabel *S-Box*.

1F	0D	07	1A
00	1C	1A	07
10	08	13	12
1C	0C	13	01

→

C0	D7	C5	A2
63	9C	A2	C5
CA	30	7D	C9
9C	FE	7D	7C

   b. Transformasi berikutnya adalah *ShiftRows*, baris pertama tidak ada pergeseran, baris kedua dilakukan pergeseran 1 *byte*, pada baris ketiga digeser 2 *byte* dan baris keempat digeser 3 *byte* ke kiri.



c. Selanjutnya adalah proses *MixColumns*, dimana proses ini akan melakukan perkalian antara bilangan *polynomial* tetap dengan *state* hasil dari *ShiftRows*.

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

x

C0	D7	C5	A2
9C	A2	C5	63
7D	C9	CA	30
7C	9C	FE	7D

=

25	1D	F1	B7
18	54	EF	49
22	43	96	26
41	2A	BC	54

d. Tranformasi akhir dari *round* ke-1 adalah *AddRoundKey*, hasil dari *MixColumns* akan di XOR-kan dengan *RoundKey* ke-1, seperti dibawah ini.

25	1D	F2	B7
18	54	EF	49
22	43	96	26
41	2A	BC	54

⊕

71	3D	74	3A
CA	81	D2	9B
06	4F	1D	5C
67	2A	6B	23

=

54	20	85	8B
D2	D5	3D	D2
24	0C	8B	7A
25	00	D7	77

Proses diatas akan diulangi untuk *round* ke-2 sampai dengan *round* ke-10. Namun, pada *round* ke 10 transformasi *MixColumns* tidak lagi dilakukan. Berikut hasil transformasi proses enkripsi:

Round ke-2

SubBytes

20	B7	97	5D
B5	03	27	B5
36	FE	3D	DA
3F	63	0E	F5

ShiftRows

20	B7	97	5D
03	27	B5	B5
3D	DA	36	FE
F5	3F	63	0E

MixColumn

8D	F9	A4	8E
94	B3	DF	3B
5D	7E	EB	1D
AF	41	E7	B0

RoundKey ke-2

67	54	2E	14
80	01	D3	48
20	6F	72	23
E7	CD	A6	85

AddRoundKey

EA	A3	BA	9A
14	B2	0C	73
7D	11	99	33
48	8C	41	35

…….

Round ke-10

SubBytes

A8	98	68	03
1C	E7	6D	6F
8B	61	FA	FD
35	30	96	F3

ShiftRows

A8	9B	68	03
E7	6D	6F	1C
FA	FD	8B	61
F3	3A	30	96

RoundKey ke-10

39	86	71	0D
7D	73	A6	D0
B8	71	E2	F9
21	1E	1E	A9

AddRoundKey

91	1D	19	0E
9A	1E	C9	CC
42	8C	69	98
D2	2B	2E	3F

1.3.3 Dekripsi

Proses dekripsi dilakukan untuk mengembalikan data yang telah dienkripsi menjadi *plaintext* kembali. Transformasi deskripsi pada algoritma *advanced encryption standard* adalah *InvSubBytes, InvShiftRows, InvMixColumns, dan AddRoundKey*[7].

Berikut adalah proses dekripsi chipertext

1. Melakukan proses XOR antara *ciphertext* dengan RoundKey ke-10.

EC	F6	C2	DC
A7	32	AD	58
E7	DA	45	00
31	E9	38	07

⊕

35	11	F2	B2
A4	6A	D7	6B
D5	6D	94	8F
5B	2D	C2	27

=

D9	E7	30	6E
03	58	7A	33
32	B7	D1	8F
6A	C4	FA	20

2. Selanjutnya, Pada *round* ke-1 sampai *round* ke-9 proses dekripsi dilakukan transformasi *InvShiftRows, InvSubBytes*, *InvMixColumns* dan *AddRoundKey*.

Round ke-1

InvShiftRows

A8	9B	68	03
E7	6D	6F	1C
FA	FD	8B	61
F3	35	30	96

→

A8	9B	68	03
1C	E7	6D	6F
8B	61	FA	FD
35	30	96	F3

3. Kemudian, lakukan proses *InvSubBytes*. Untuk S-Box *InvSubBytes* berbeda dengan S-BOX *SubBytes* karena telah dilakukan *invers* namun, cara kerjanya sama.

A8	98	68	03
1C	E7	6D	6F
8B	61	FA	FD
35	30	96	F3

→

6F	E8	F7	D5
CF	B0	B3	06
CE	D8	14	21
D9	08	35	7E

4. Melakukan proses XOR antara *InvSubBytes* dengan *RoundKey* ke- 9.

6F	E8	F7	D5	⊕	37	BF	F7	7C	=	58	57	00	A9
CF	B0	B3	06		D2	0F	D5	76		16	BE	66	70
CE	D8	14	21		11	C9	93	1B		DF	11	87	3A
D9	08	35	7E		31	3F	00	B7		E8	37	35	39

5. Selanjutnya, melakukan proses transformasi antara hasil *AddRoundKey* dengan dot product dengan mengikuti aturan *irreducible polynomial*.

0E	0B	0D	09	⊕	58	57	00	A9	=	72	70	C8	1B
09	0E	0B	0D		16	BE	66	70		D6	04	C6	57
0D	09	0E	0B		DF	11	87	3A		07	B3	FC	DC
0B	0D	09	0E		E8	37	35	39		DA	08	26	BA

Proses di atas akan diulangi untuk mendapatkan hasil transformasi *round* ke-2 sampai dengan *round* ke-10, seperti yang di bawah ini :

Round ke-2

InvShiftRows

72	70	CB	1B
57	D6	04	C6
FC	DC	07	B3
08	26	BA	DA

InvSubBytes

1E	D0	B1	44
DA	4A	30	3C7
55	93	38	4B
BF	23	C0	7A

RoundKey ke-8

26	88	48	8B
16	DC	DB	A3
B8	D8	5A	88
0C	0E	3F	B7

AddRoundKey

38	58	F9	CF
CC	96	EB	64
ED	48	62	C3
B3	2D	FF	CD

InvMixColumn

3F	0C	1C	48
E4	72	29	59
A5	54	82	15
D4	82	38	A1

……..

Round ke-10

InvShiftRows

C0	D7	C5	A2
52	9C	A2	C5
CA	30	7D	C9
9C	FE	7D	7C

InvSubBytes

1F	0D	07	1A
00	1C	1A	07
10	08	13	12
1C	0C	13	01

RoundKey ke-0

67	5A	2E	14
80	01	D3	48
20	6F	72	23
E7	CD	A6	85

AddRoundKey

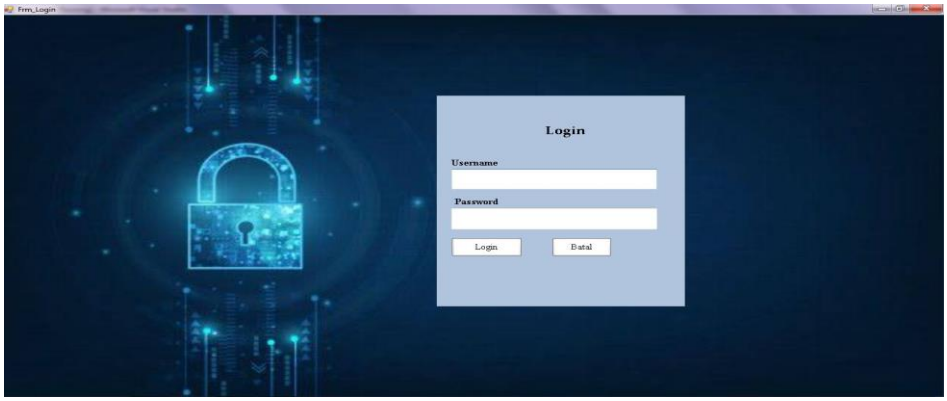
54	41	4E	54
49	57	49	4E
44	41	41	53
54	41	52	49

Hasil dari proses dekripsi yaitu: 54414E544957494E4441415354415249.

3. ANALISA DAN HASIL

3.1 Tampilan *Form Login*

Tampilan menu *login* adalah tampilan untuk masuk ke menu utama. *User* melakukan *login* terlebih dahulu dengan cara menginput *username* dan *password* dengan benar sesuai dengan *database*. Berikut ini adalah menu *login* :



Gambar 3.1 Tampilan *Form Login*

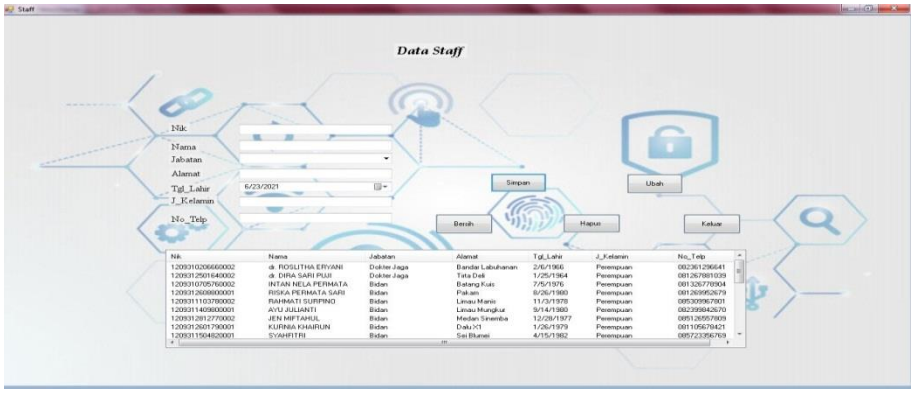
3.2 *Form* Menu Utama

Menu Utama merupakan *form* yang akan menampilkan menu pada sistem. Menu Utama terdiri dari beberapa tombol yaitu Menu Data Staff, Menu Data Gaji, Menu Enkripsi dan Dekripsi. Berikut adalah tampilan Menu Utama :

Gambar 3.2 *Form Menu Utama*

3.3 *Form* Data Staff

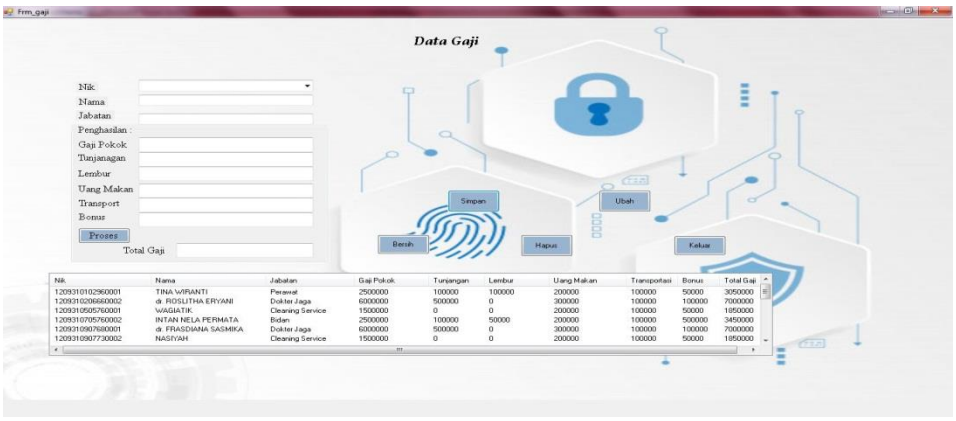
Form ini digunakan untuk mengelolah data staff. Adapun tampilan data staff sebagai berikut :



Gambar 3.3 *Form* Data Staff

3.4 *Form* Data Gaji

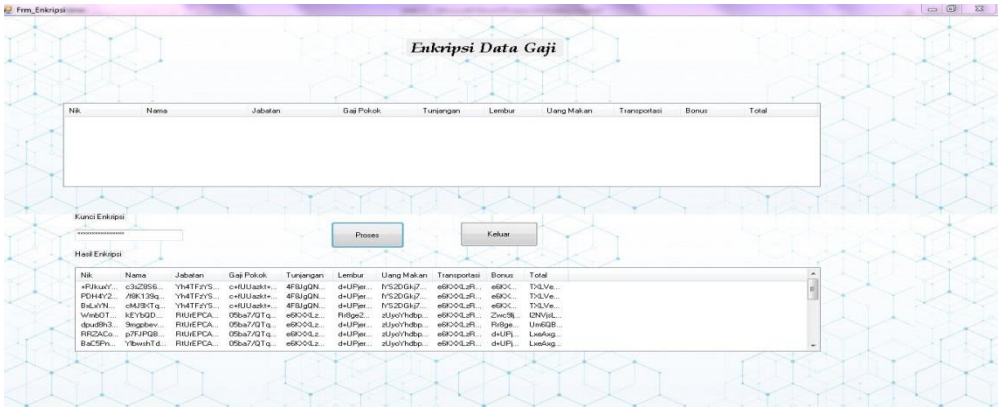
Form ini digunakan untuk mengelolah data gaji karyawan berdasarkan status jabatan. Berikut ini tampilan dari *form* Data Gaji.



Gambar 3.4 *Form* Data Gaji

3.5 *Form* Enkripsi

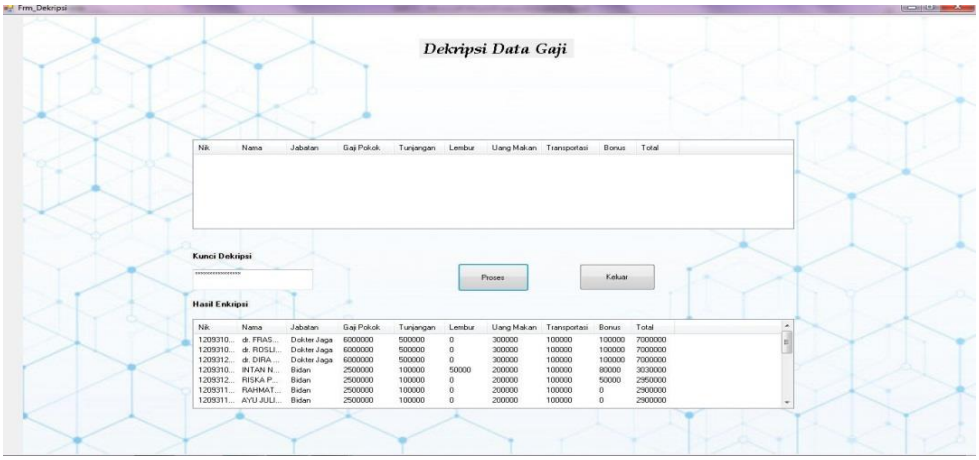
Form enkripsi digunakan untuk melakukan proses penyandian pada data. Berikut tampilan dari *form* enkripsi :



Gambar 3.5 *Form* Enkripsi

3.6 *Form* Dekripsi

Form ini digunakan untuk mengembalikan data yang sudah di sandi kebentuk semula agar dapat dibaca. Berikut tampilan dari *form* Dekripsi.



Gambar 3.6 *Form* Dekripsi

4. KESIMPULAN

Berdasarkan Penelitain yang telah dilakukan dalam tahap perancangan dan evaluasi implementasi kriptografi data gaji pada Klinik Pratama Siti Rahmah, menggunakan metode *Advanced Encryption Standard* (AES) berhasil diterapkan.

Pengimplementasi AES dilakukan dengan biner maupun hexsa, data yang sudah terenkripsi tidak dapat dibaca sebelum data tersebut didekripsi atau di ubah menjadi *plaintext* sehingga data tersebut dapat dibaca kembali.

UCAPAN TERIMA KASIH

Pada kesempatan ini penulis mengucapkan banyak terimakasih kepada kedua orang tua yang telah banyak memberikan dukungan moril dan materil, tidak terkecuali doa yang senantiasa dipanjatkan sehingga penulis dapat menyelesaikan penelitian ini.

Penyusunan jurnal ini juga tidak terlepas dari bantuan berbagai pihak. Oleh karena itu dengan segala kerendahan hati, diucapkan terimakasih yang sebesar-besarnya kepada: Bapak Azanuddin,S.Kom.,M.Kom selaku Dosen Pembimbing I, kepada Ibu Vina Winda Sari S.E,M.Ak selaku Dosen Pembimbing II yang telah banyak membantu dalam memberikan arahan dan bimbingan.

REFERENSI

[1] I. A. Susanto *et al.*, "ENKRIPSI DATA PENGGAJIAN DENGAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER PADA PT . KEMASINDO CEPAT NUSANTARA," vol. 1, no. 1, pp. 399–404, 2018.

[2] W. Ariandi, S. Widyastuti, and L. Haris, "Implementasi Block Cipher Electronic Codebook (ECB) untuk Pengamanan Data Pegawai," *J. Ilm. Intech Inf. Technol. J. UMUS*, vol. 2, no. 02, pp. 65–74, 2020, doi: 10.46772/intech.v2i02.291.

[3] R. Munir, *Kriptografi*. Informatika Bandung, 2019.

[4] H. Madora, I. Wahyuningrum, and M. Noval, "Perancangan Program Aplikasi Peminjaman dan Pengembalian Buku di Ruang Baca Jurusan Manajemen Informatika Politeknik Negeri Sriwijaya," vol. 13, no. 2, pp. 113–121, 2019.

[5] I. J.Prayudha,Saniman, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," vol. 18, no. SAINTIKOM, pp. 119–129, 2019.

[6] A. A. Ibrahim, "Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)," *J. Tek. Inform. STMIK Antar Bangsa*, vol. 3, no. 1, pp. 53–60, 2017, [Online]. Available: https://ejournal.antarbangsa.ac.id/index.php/jti/article/view/131.

[7] A. S. Agung Prajuanaputra, Herfina, Supiatul Maryana, "implementasi algoritma aes (advanced Encryption Standard) Rijendael pada Aplikasi Keamanan Data," vol. 1, pp. 46–51, 2020.

BIBLIOGRAFI PENULIS

Nama : Nabilah Qomariah Dolok Saribu
Tempat/Tgl : Medan, 28 April 1998
Alamat : Teluk Dalam, Asahan
Agama : Islam
Jenis Kelamin : Perempuan
No.Hp : 0853-6126-6115
Bidang Keilmuan : Kriptografi dan Desain Grafis
E-mail : qomariahnabilah2804@gmail.com

Nama : Azanuddin, S.Kom., M.Kom
Tempat/Tgl : Klambir Lima, 26 Juni 1989
Alamat : Dusun XI Gg. Mardisan
Agama : Islam
Jenis Kelamin : Laki-Laki
No.Hp : 0813-7683-7222
Prestasi Dosen : -
Bidang Keilmuan : Jaringan, Mobile, dan Sistem Terdistribusi
Email : azdin.bpc@gmail.com

Nama : Vina Winda Sari, S.E.M.Ak
Tempat/Tgl : Medan, 19 Juni 1984
Alamat : Jl.Pinang Baris Gg.Keluarga No.145 H Lk.1
Agama : Islam
Jenis Kelamin : Perempuan
No.Hp : 0813-7625-6397
Prestasi Dosen : -
Bidang Keilmuan : Akuntansi
Email : winda_vina@yahoo.co.id