

METODE AES DALAM MENGAMANKAN DATA KARYAWAN PADA PT. JAYA BIRAWA KALOKA

Azizi Ananda Putra¹, Nidia Enjelita Br Saragih²

^{1,2}Teknik Dan Ilmu Komputer, Informatika, Universitas Potensi utama

E-mail: aziziputra192@gmail.com¹, nidia.1924@gmail.com²

ABSTRAK

PT. Jaya Birawa Kaloka (JBK) memiliki masalah yaitu sering hilangnya data penting yang disebabkan oleh kurangnya keamanan terhadap data absensi penting tersebut. Hilangnya data penting dapat terjadi melalui beberapa hal salah satunya yaitu proses absensi karyawan dilakukan secara manual. Kendala lainnya adalah kurangnya kebijakan keamanan yang jelas, sistem yang berjalan tidak memadai untuk atau using, Kurangnya Pengawasan terhadap akses data, penyimpanan data yang tidak aman, kebijakan pengelolaan data yang tidak memadai, kurangnya pelatihan keamanan untuk karyawan, serangan siber dan keamanan yang lemah, kurangnya pengawasan internal dan audit dan kepatuhan terhadap regulasi yang lemah. Oleh karena itu dibutuhkan sebuah sistem yang difokuskan mampu menjaga keamanan data penting yang ada diperusahaan dari ancaman orang yang tidak bertanggung jawab. AES adalah sebuah algoritma enkripsi simetris yang digunakan untuk mengamankan data dalam bentuk digital. Algoritma ini terdiri dari beberapa jenis kunci enkripsi yang berbeda, yang masing-masing memiliki panjang bit yang berbeda. AES telah terbukti efektif dalam menjaga kerahasiaan dan keamanan data, sehingga sering digunakan pada sistem keamanan data dan aplikasi (Pabokory et al., 2020)

Kata Kunci: Keamanan data, Karyawan, AES, Web

ABSTRACT

PT. Jaya Birawa Kaloka (JBK) has a problem, namely the frequent loss of important data caused by a lack of security for important attendance data. Loss of important data can occur through several things, one of which is the employee attendance process being carried out manually. Other obstacles are the lack of a clear security policy, inadequate or outdated systems, lack of supervision over data access, insecure data storage, inadequate data management policies, lack of security training for employees, cyber attacks and weak security, lack of internal monitoring and auditing and weak regulatory compliance. Therefore, we need a system that is focused on being able to maintain the security of important data in the company from threats from irresponsible people. AES is a symmetric encryption algorithm used to secure data in digital form. This algorithm consists of several different types of encryption keys, each of which has a different bit length. AES has been proven effective in maintaining data confidentiality and security, so it is often used in data and application security systems (Pabokory et al., 2020)

Keywords: Data security, Employees, AES, Web

I. PENDAHULUAN

Keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting (Denny Ardianta Sitepu, 2022).

PT. Jaya Birawa Kaloka (JBK) adalah Badan Usaha Berbadan Hukum yang bergerak pada bidang jasa penyedia sumber daya manusia (SDM Alih Daya) Outsourcing dan Manajemen Fungsi Sumber Daya Manusia. Dengan misinya yaitu untuk menjadi perusahaan terkemuka, yang mampu memberikan rasa aman dan manfaat optimal kepada semua pihak yang berkepentingan. PT. Jaya Birawa Kaloka (JBK) memiliki masalah yaitu sering hilangnya data penting yang disebabkan oleh kurangnya keamanan terhadap data absensi penting tersebut khususnya data absensi karyawan. Proses absensi karyawan masih dilakukan dengan cara manual yaitu menggunakan rekapan buku baik untuk jadwal masuk kerja dan pulang kerja. Hal tersebut mengakibatkan hilangnya data absensi karyawan dan tidak dapat terjaga untuk data absensi karyawan. Kendala lainnya adalah kurangnya kebijakan keamanan yang jelas, sistem yang berjalan tidak memadai untuk atau using, Kurangnya Pengawasan terhadap akses data, penyimpanan data yang tidak aman, kebijakan pengelolaan data yang tidak memadai, kurangnya pelatihan keamanan untuk karyawan, serangan siber dan keamanan yang lemah, kurangnya pengawasan internal dan audit dan kepatuhan terhadap regulasi yang lemah. Hilangnya data penting dapat terjadi melalui beberapa hal salah satunya yaitu berbagi file absensi sembarangan. Data absensi karyawan dibutuhkan untuk mengetahui apakah seorang karyawan datang dan meninggalkan kantor sesuai dengan jam kerja yang telah di tentukan atau tidak. selain itu absensi juga dibutuhkan untuk mengetahui apakah seorang karyawan bekerja lembur atau tidak, dan oleh sebab itu PT. Jaya Birawa Kaloka (JBK) juga harus lebih meningkatkan keamanan data absensi harian karyawan agar tidak terjadi hal - hal yang tidak diinginkan Maka di butuhkan sebuah metode penyandian, ilmu sekaligus seni guna menjaga informasi yang disebut juga dengan Kriptografi.

Untuk mengatasi permasalahan tersebut, penulis membuat program aplikasi pengamanan data absensi karyawan dengan menggunakan teknologi informasi yang berbasis web yaitu kriptografi. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan cara mengubahnya menjadikan kode tertentu dan hanya di

tujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi untuk menjaga kerahasiaan data atau pesan. dalam kriptografi, data atau pesan yang di kirimkan melalui jaringan akan di samarkan sedemikian rupa. Sehingga seandainya data tersebut dapat di peroleh dan di baca oleh orang lain, maka pihak yang tidak berhak dan berwenang tidak akan dapat mengerti arti dari data tersebut dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu Enskripsi dan Dekripsi .Enskripsi adalah proses dimana informasi atau data yang hendak di kirim di ubah menjadi bentuk yang hampir di kenal sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk yang tersamar tersebut menjadi informasi awal. sebuah pesan atau data yang masih asli dan belum mengalami penyandian di kenal dengan istilah plaintext . Salah satu metode kriptografi yang digunakan dalam pengamanan data absensi adalah metode AES (*Advanced Encryption Standard*) (Arief Anrico Pandiangan : 2021)

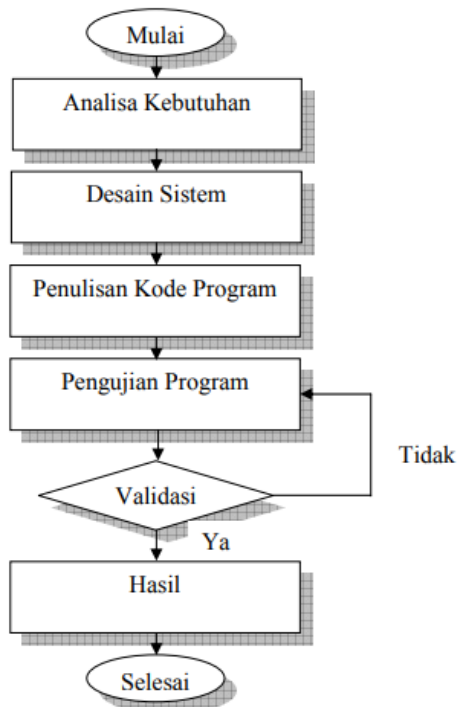
Algoritma AES digunakan untuk mengenkripsi dan deskripsi informasi, yang menggunakan proses yang berulang. Selain itu AES lebih efisien dari segi biaya dan lebih mudah diimplementasikan pada memori berukuran kecil (Halomoan & Yunita, 2022).

Pada algoritma AES dalam melakukan enkripsi sebuah data, terdapat perhitungan matematis di dalamnya. Perhitungan tersebut adalah penjumlahan dan perkalian. Hal ini dikarenakan perhitungan algoritma kriptografi AES berbeda dengan perhitungan matematis pada umumnya. Oleh karena itulah, penelitian ini akan mengenalkan AES sebagai salah satu algoritma kriptografi dalam melakukan pengamanan data dengan perhitungan matematis (Nur Wachid Hidayatulloh : 2023).

Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut plainteks. Disebut demikian karena informasi ini dapat dengan mudah dibaca dan dipahami oleh siapa saja. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi plainteks melibatkan penggunaan beberapa bentuk kunci (Muhammad Azhari, 2022).

II. METODE PENELITIAN

Berikut adalah alir diagram metode penelitian yang digunakan dalam penulisan skripsi ini :

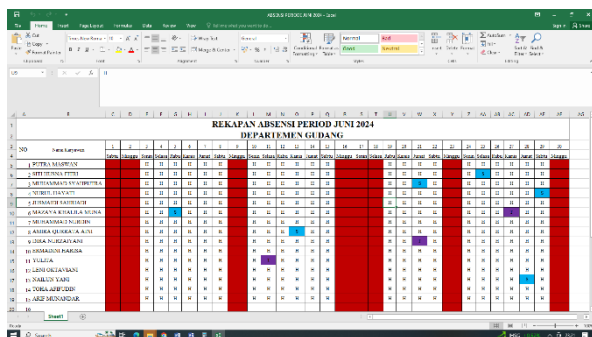


Gambar 1. Diagram Alir Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini peneliti mengumpulkan data-data yang berkaitan dengan penelitian. Peneliti juga menentukan *software* dan *hardware* yang akan digunakan untuk membuat penelitian. Berikut ini merupakan data laporan absensi keuangan pada PT. Jaya Birawa Kaloka (JBK):



NO	Nama Karyawan	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	PITRA SURYON																															
2	ADRI WISNU PRATI																															
3	MARTINDA SYAHRIYATI																															
4	NURUL HANIKI																															
5	PRATIWIYATI KURNIAWATI																															
6	ANAKYA A. PARADA SIKHA																															
7	MELANINGSI NURBIRI																															
8	ANANDA SIKHA R. KASU																															
9	ALONA N. RIZKIANI																															
10	BERNARDINO PARKISA																															
11	RI YULIA																															
12	LEONOR LAKSANA																															
13	DIANESDI YANI																															
14	DENISA ARIYUSDI																															
15	ANZ MURNIDAR																															

Gambar 2. Absensi Karyawan Pada PT. Jaya Birawa Kaloka (JBK)

2. Desain Sistem

Untuk mendesain sistem peneliti menggunakan beberapa pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Dalam penulisan kode program, peneliti menggunakan bahasa pemrograman PHP.

4. Pengujian Program

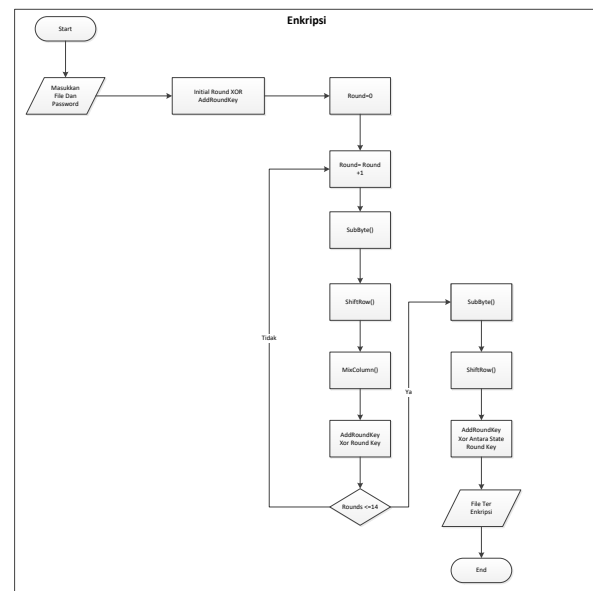
Pengujian program dilakukan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik. Pengujian dengan teori menggunakan blackbox testing dan pengujian dengan praktek menggunakan Java

5. Hasil

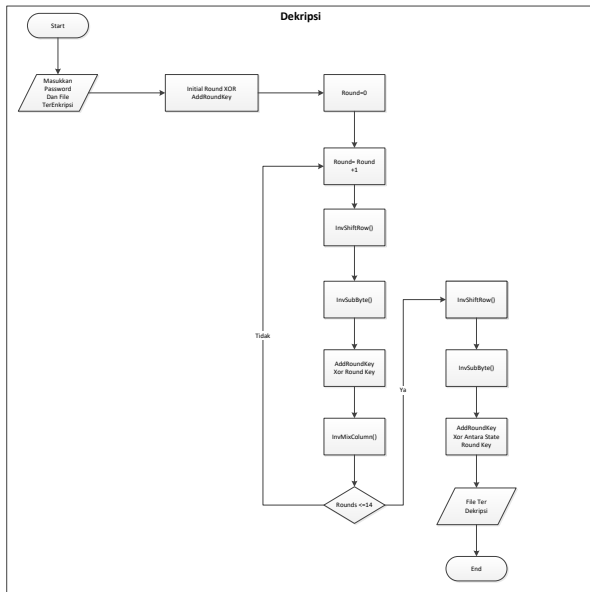
Pada tahapan ini aplikasi keamanan data karyawan menggunakan metode AES sudah dapat berjalan dengan baik dan penelitian ini menghasilkan pemahaman mengenai metode AES

III. HASIL DAN PEMBAHASAN

Langkah yang harus dilakukan dalam proses enkripsi dan dekripsi digambarkan dalam flowchart berikut :



Gambar 3. Flowchart Enkripsi AES



Gambar 4. Flowchart Dekripsi AES

Berikut ini adalah contoh kasus penggunaan Algoritma AES, untuk lebih jelasnya dapat dilihat sebagai berikut :

Misal, sebuah CipherText sebagai berikut :
 CipherText : BudiSuhartono
 Key : Jbirawakaloka

Langkah selanjutnya adalah mengubah nama file dan juga kunci kedalam bentuk hexadesimal.

File :

B	U	D	I	S	U	H	A	R	T	O	N	O
5	7	6	4	6	6	4	6	6	6	5	7	6
4	7	F	F	E	5	E	9	E	5	4	7	F

Key :

J	B	I	R	A	W	A	K	A	L	O	K	A
5	6	6	7	7	4	7	4	7	6	6	4	7
4	8	1	4	3	D	9	B	5	E	7	6	5

Langkah selanjutnya yang dilakukan adalah mencari nilai Roundkey pertama, untuk mencari Roundkey pertama dapat dilakukan sebagai berikut :

w[0] = (54, 68, 61, 74)

w[1] = (73, 20, 6D, 79)

w[2] = (20, 4B, 75, 6E)

w[3] = (67, 20, 46, 75)

g(w[3]) :

- byte kiri bergeser dari w[3] : (20, 46, 75, 67)
- Substitusi Byte (S-Box): (B7, 5A, 9D, 85)
- Menambahkan putaran konstan (01, 00, 00, 00)
- Memberi : g(w[3]) = (B6, 5A, 9D, 85)

w[4] = w[0] g(w[3]) = (E2, 32, FC, F1) :

0101 0100	0110 1000	0110 0001	0111 0100
-----------	-----------	-----------	-----------

1011 0110	0101 1010	1001 1101	1000 0101
1110 0010	0011 0010	1111 1100	1111 0001
E2	32	FC	F1

w[5] = w[4] XOR w[1] = (91, 12, 91, 88)

w[6] = w[5] w[2] = (B1, 59, E4, E6)

w[7] = w[6] w[3] = (D6, 79, A2, 93)

Roundkey pertama : E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

Round0 : 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Round1 : E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79

Round2 : 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA

Round3 : D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03

Round4 : A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B

Round5 : B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69

Round6 : BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E

Round7 : CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A

Round8 : 8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C

Round9 : BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8

Round10 : 28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

Pertama dilakukan proses inisialisasi dengan operasi XOR antara State dan Key.

State Matrix dan Round key No.0 Matrix :

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \quad \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix}$$

XOR entri yang sesuai, misalnya, 69 XOR 4B = 22

0110 1001

0100 1011

0010 0010

State Matrix baru adalah :

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

Gantikan setiap entri (byte) dari matriks keadaan saat ini dengan entri yang sesuai di AES S-Box. Misalnya : byte 6E diganti dengan masuknya S-Box di baris 6 dan kolom E, yaitu, oleh 9F. Ini mengarah ke Matriks Status baru :

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

Lapisan non-linear ini untuk ketahanan terhadap serangan kriptanalisis yang berbeda dan linier. empat baris digeser secara siklis ke kiri dengan offset 0,1, 2, dan 3. State Matrix baru adalah :

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

Langkah pencampuran linier ini menyebabkan difusi bit pada beberapa putaran. Campur Kolom mengalikan matriks tetap terhadap Matriks Status saat ini :

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

Entri BA adalah hasil dari (02x63) XOR (03x2F) XOR (01xAF) XOR (01xA2) :
 $02 \times 63 = 00000010 \times 01100011 = 11000110$

$$03 \times 2F = (02 \times 2F) \text{ XOR } 2F = (00000010 \times 00101111) \text{ XOR } 00101111 = 01110001$$

$$01 \times AF = AF = 10101111 \text{ dan } 01 \times A2 = A2 = 10100010$$

Dikarenakan :

$$\begin{matrix} 11000110 \\ 01110001 \\ 10101111 \\ 10100010 \end{matrix}$$

$$10111010$$

State Matrix dan Round key No.1 Matrix:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \quad \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix}$$

XOR menghasilkan Matriks Status baru:

$$\begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

Output AES setelah Putaran 1: 58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE

Putaran 2 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 6A & 59 & CB & BD \\ A0 & 4E & 48 & 12 \\ 30 & 9C & 98 & 9E \\ 3D & F4 & 9B & 8B \end{pmatrix} \quad \begin{pmatrix} 6A & 59 & CB & BD \\ 4E & 48 & 12 & A0 \\ 98 & 9E & 30 & 9B \\ 8B & 3D & F4 & 9B \end{pmatrix}$$

Putaran 2 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 15 & C9 & 7F & 9D \\ CE & 4D & 4B & C2 \\ 89 & 71 & BE & 88 \\ 65 & 47 & 97 & CD \end{pmatrix} \quad \begin{pmatrix} 43 & 0E & 09 & 3D \\ C6 & 57 & 08 & F8 \\ A9 & C0 & EB & 7F \\ 62 & C8 & FE & 37 \end{pmatrix}$$

Putaran 3 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 1A & AB & 01 & 27 \\ B4 & 5B & 30 & 41 \\ D3 & BA & E9 & D2 \\ AA & E8 & BB & 9A \end{pmatrix} \quad \begin{pmatrix} 1A & AB & 01 & 27 \\ 5B & 30 & 41 & B4 \\ E9 & D2 & D3 & BA \\ A9 & AA & E8 & BB \end{pmatrix}$$

Putaran 3 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} AA & 65 & FA & 88 \\ 16 & 0C & 05 & 3A \\ 3D & C1 & DE & 2A \\ B3 & 4B & 5A & 0A \end{pmatrix} \quad \begin{pmatrix} 78 & 70 & 99 & 4B \\ 76 & 76 & 3C & 39 \\ 30 & 7D & 37 & 34 \\ 54 & 23 & 5B & F1 \end{pmatrix}$$

Putaran 4 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} BC & 51 & EE & B3 \\ 38 & 38 & EB & 12 \\ 04 & FF & 9A & 18 \\ 20 & 26 & 39 & A1 \end{pmatrix} \quad \begin{pmatrix} BC & 51 & EE & B3 \\ 38 & EB & 12 & 38 \\ 9A & 18 & 04 & FF \\ A1 & 20 & 26 & 39 \end{pmatrix}$$

Putaran 4 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 10 & BC & D3 & F3 \\ D8 & 94 & E0 & E0 \\ 53 & EA & 9E & 25 \\ 24 & 40 & 73 & 7B \end{pmatrix} \quad \begin{pmatrix} B1 & 08 & 04 & E7 \\ CA & FC & B1 & B2 \\ 51 & 54 & C9 & 6C \\ ED & E1 & D3 & 20 \end{pmatrix}$$

Putaran 5 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} C8 & 30 & F2 & 94 \\ 74 & B0 & C8 & 37 \\ D1 & 20 & DD & 50 \\ 55 & F8 & 66 & B7 \end{pmatrix} \quad \begin{pmatrix} C8 & 30 & F2 & 94 \\ B0 & C8 & 37 & 74 \\ DD & 50 & D1 & 20 \\ B7 & 55 & F8 & 66 \end{pmatrix}$$

Putaran 5 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 2A & 26 & 8F & E9 \\ 78 & 1E & 0C & 7A \\ 1B & A7 & 6F & 0A \\ 5B & 62 & 00 & 3F \end{pmatrix} \quad \begin{pmatrix} 9B & 23 & 5D & 2F \\ 51 & 5F & 1C & 38 \\ 20 & 22 & BD & 91 \\ 68 & F0 & 32 & 56 \end{pmatrix}$$

Putaran 6 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 14 & 26 & 4C & 15 \\ D1 & CF & 9C & 07 \\ B7 & 93 & 7A & 81 \\ 45 & 8C & 23 & B1 \end{pmatrix} \quad \begin{pmatrix} 14 & 26 & 4C & 15 \\ CF & 9C & 07 & D1 \\ 7A & 81 & B7 & 93 \\ B1 & 45 & 8C & 23 \end{pmatrix}$$

Putaran 6 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} A9 & 37 & AA & F2 \\ AE & D8 & 0C & 21 \\ E7 & 6C & B1 & 9C \\ F0 & FD & 67 & 3B \end{pmatrix} \quad \begin{pmatrix} 14 & 8F & C0 & 5E \\ 93 & A4 & 60 & 0F \\ 25 & 2B & 24 & 92 \\ 77 & E8 & 40 & 75 \end{pmatrix}$$

Putaran 7 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} FA & 73 & BA & 58 \\ DC & 49 & D0 & 76 \\ 3F & F1 & 36 & 4F \\ F5 & 9B & 09 & 9D \end{pmatrix} \quad \begin{pmatrix} FA & 73 & BA & 58 \\ 49 & D0 & 76 & DC \\ 36 & 4F & 3F & F1 \\ 9D & F5 & 9B & 09 \end{pmatrix}$$

Putaran 7 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 9F & 37 & 51 & 37 \\ AF & EC & 8C & FA \\ 63 & 39 & 04 & 66 \\ 4B & FB & B1 & D7 \end{pmatrix} \quad \begin{pmatrix} 53 & 43 & 4F & 85 \\ 39 & 06 & 0A & 52 \\ 8E & 93 & 3B & 57 \\ 5D & F8 & 95 & BD \end{pmatrix}$$

Putaran 8 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} ED & 1A & 84 & 97 \\ 12 & 6F & 67 & 00 \\ 19 & DC & E2 & 5B \\ 4C & 41 & 2A & 7A \end{pmatrix} \quad \begin{pmatrix} ED & 1A & 84 & 97 \\ 6F & 67 & 00 & 12 \\ E2 & 5B & 19 & DC \\ 7A & 4C & 41 & 2A \end{pmatrix}$$

Putaran 8 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} E8 & 8A & 4B & F5 \\ 74 & 75 & EE & E6 \\ D3 & 1F & 75 & 58 \\ 55 & 8A & 0C & 38 \end{pmatrix} \quad \begin{pmatrix} 66 & 70 & AF & A3 \\ 25 & CE & D3 & 73 \\ 3C & 5A & 0F & 13 \\ 74 & A8 & 0A & 54 \end{pmatrix}$$

Putaran 9 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 33 & 51 & 79 & 0A \\ 3F & 8B & 66 & 8F \\ EB & BE & 76 & 7D \\ 92 & C2 & 67 & 20 \end{pmatrix} \quad \begin{pmatrix} 33 & 51 & 79 & 0A \\ 8B & 66 & 8F & 3F \\ 76 & 7D & EB & BE \\ 20 & 92 & C2 & 67 \end{pmatrix}$$

Putaran 9 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & FB \\ E8 & D7 & 70 & 51 \end{pmatrix} \quad \begin{pmatrix} 09 & A2 & F0 & 7B \\ 66 & D1 & FC & 3B \\ 8B & 9A & E6 & BE \\ 78 & 65 & C4 & 89 \end{pmatrix}$$

Putaran 10 setelah Pengganti Byte dan setelah Shift Rows:

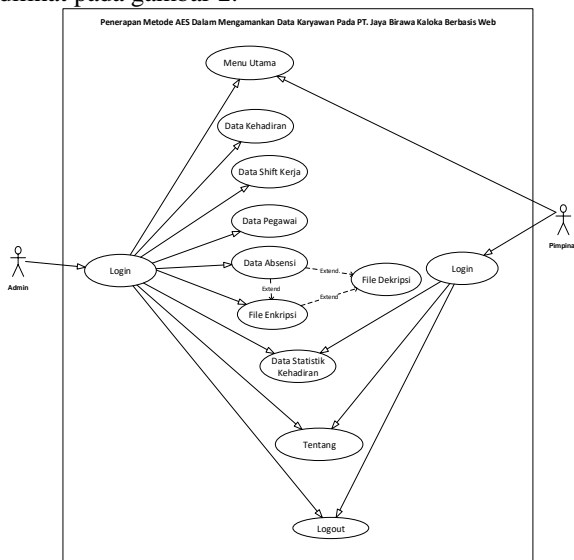
$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & A7 \end{pmatrix} \quad \begin{pmatrix} 01 & 3A & 8C & 21 \\ E3 & B0 & E2 & 33 \\ 8E & 04 & 3D & 8C \\ A7 & BC & 4D & 1C \end{pmatrix}$$

Putaran 10 setelah Roundkey (Perhatian: tidak ada kolom Mix di round terakhir):

$$\begin{pmatrix} 29 & 57 & 40 & 1A \\ C3 & 14 & 22 & 02 \\ 50 & 20 & 99 & D7 \\ 5F & F6 & B3 & 3A \end{pmatrix}$$

Cipher File yang dihasilkan adalah sebagai berikut :
29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

Sebuah use case digambarkan sebagai elips horizontal dalam suatu diagram UML use case, dapat dilihat pada gambar 2:

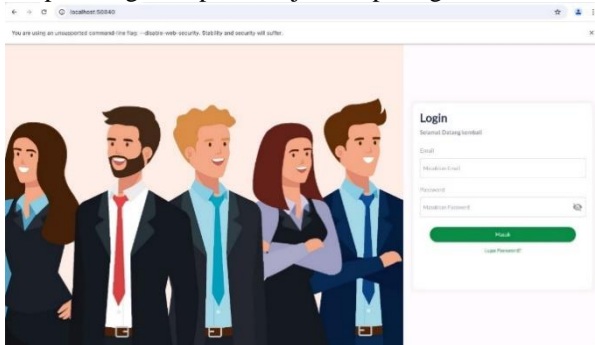


Gambar 5. Use Case Diagram

Tampilan Hasil

1. Tampilan Menu login

Tampilan beranda merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai form login admin program. Gambar tampilan login dapat ditunjukkan pada gambar 7 :

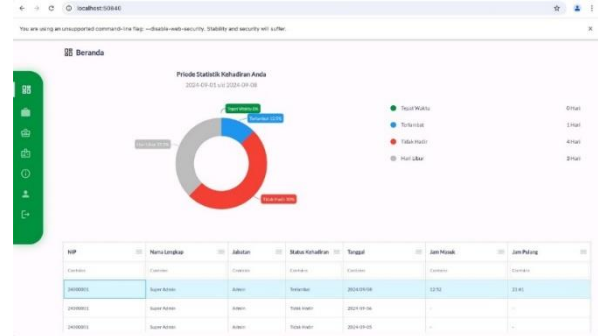


Gambar 7. Tampilan Form Login

2. Tampilan Menu beranda

Tampilan beranda merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai form beranda admin program.

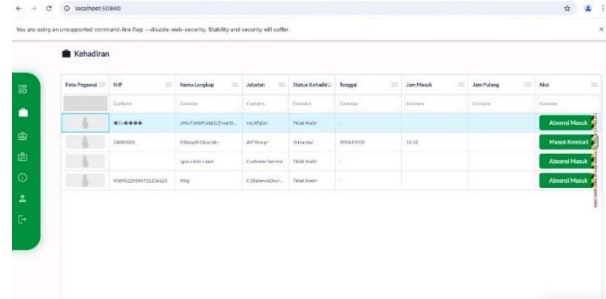
Gambar tampilan beranda dapat ditunjukkan pada gambar 8 :



Gambar 8. Tampilan Form Beranda

3. Tampilan Form data kehadiran Pegawai

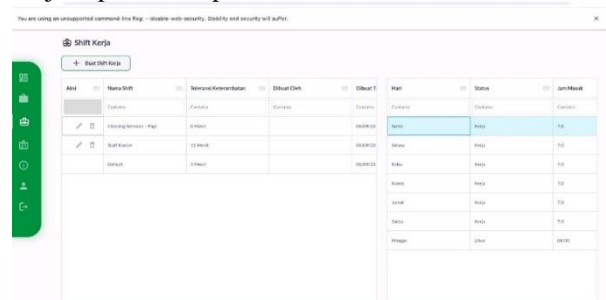
Form utama merupakan interface program menu kehadiran pegawai, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui interface form menu kehadiran pegawai. Dalam form menu kehadiran pegawai terdapat beberapa menu yaitu, menu file dan menu program. Untuk lebih jelasnya tampilan form menu kehadiran pegawai dapat dilihat pada Gambar 9 dibawah ini.



Gambar 9. Tampilan Form Menu Kehadiran Pegawai

4. Tampilan Form data Shift Kerja

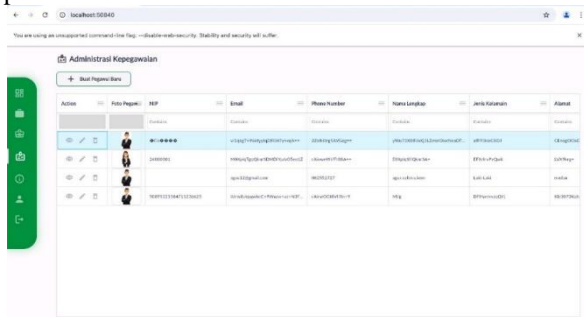
Form utama merupakan interface program menu shift kerja, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui interface form menu shift kerja. Untuk lebih jelasnya tampilan form menu shift kerja dapat dilihat pada Gambar 10 dibawah ini.



Gambar 10. Tampilan Form Menu Shift Kerja

5. Tampilan Form data Pegawai

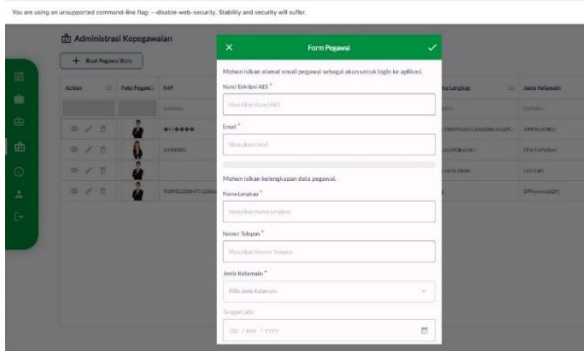
Form utama merupakan *interface* program menu pegawai, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* menu pegawai. Dalam *form* menu pegawai terdapat beberapa menu yaitu, menu *file* dan menu program. Untuk lebih jelasnya tampilan *form* menu pegawai dapat dilihat pada Gambar 11 dibawah ini.



Gambar 11. Tampilan *Form* Menu Pegawai

6. Tampilan *Form* Data input data pegawai

Form daftar data pegawai ini berfungsi untuk merubah isi data *file* dalam bentuk *chipertext*, menyimpan hasil enkripsi (*chipertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data daftar data pegawai dapat dilihat pada gambar 12 berikut ini:



Gambar 12. Tampilan *Form* Data Input Data Pegawai

IV. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan yaitu Penerapan Metode AES Dalam Mengamankan Data Karyawan Pada PT. Jaya Birawa Kaloka Berbasis Web, dapat disimpulkan aplikasi yang sudah dirancang berbasis terkomputerisasi sehingga dapat mengatasi kendala proses absensi yang manual dan menjaga kerahasiaan data absensi pegawai.

Saran

Untuk menyempurnakan aplikasi ini maka diberikan saran :

1. Diharapkan sistem dapat dikembangkan agar sinkron dengan sistem penggajian pada PT. Jaya Birawa Kaloka.

2. Aplikasi absensi memiliki fitur konfirmasi dengan admin di lokasi perusahaan.

REFERENSI

- [1] Deppi Linda, 2019, “*Analisis Sistem Informasi Pengawas Keamanan Dan Kesehatan Makan Pada Dinas Kesehatan Kota Bandar Lampung*”
- [2] Faisal Dongoran, 2018, “*Analisis Jumlah Pengangguran Dan Ketenagakerjaan Terhadap Keberadaan Usaha Mikro Kecil Dan Menengah Di Kota Medan*” ISSN: 2442-6024
- [3] Ginantra, N. L. W. S. R., & Anandita, I. B. G. (2019). Penerapan Metode Single Exponential Smoothing Dalam Peramalan Penjualan Barang. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, 3(2), 433-441.
- [4] Gunawan, D., & Kurniawan, W. J. (2020). Perancangan Sistem Informasi Purchase Order Menggunakan Metode Single Exponential Smoothing. *Jurnal Mahasiswa Aplikasi Teknologi Komputer dan Informasi (JMApTeKsi)*, 2(1), 13-18.
- [5] Hermiati, R., Asnawati, A., & Kanedi, I. (2021). Pembuatan E-Commerce Pada Raja Komputer Menggunakan Bahasa Pemrograman Php Dan Database Mysql. *Jurnal Media Infotama*, 17(1).
- [6] Janis, J. W., Mamahit, D. J., Sugiarto, B. A., & Rumagit, A. M. (2020). Rancang bangun aplikasi online sistem pemesanan jasa tukang bangunan berbasis lokasi. *Jurnal Teknik Informatika*, 15(1), 1-12.
- [7] Kedaung, A. K. P. (2020). Penerapan Metode Single Exponential Smoothing untuk Memprediksi Penjualan Katering pada Kedai Pojok Kedaung. *Jurnal Ilmiah Intech: Information Technology Journal of UMUS*, 2(02), 35-44.
- [8] Lisnawati, N., Syafwan, H., & Nehe, N. (2022). Penerapan Metode Single Exponential Smoothing (SES) dalam Peramalan Jumlah Ikan. *Building of Informatics, Technology and Science (BITS)*, 4(2), 829-838.
- [9] Mico, A. D., Arifianto, D., & Zakriyyah, A. M. (2022). Peramalan Penjualan Batu Gamping Pada UD eko jaya menggunakan single exponential smoothing dan double exponential smoothing. *Jurnal cafetaria*, 3(2), 151-160.
- [10] Sutiyono, S. (2020). *Membangun Sistem Informasi Pendaftaran Siswa Baru Berbasis Web Dengan Metode Mdd (Model Driven Development) Di Raudhatul Athfal Nahjussalam*. *Jurnal Sistem Informasi, J-SIKA*, 2(01), 50-56.

- [11] Wahyudin, A. A. F. N., Primajaya, A., & Irawan, A. S. Y. (2020). Penerapan Algoritma Regresi Linear Berganda Pada Estimasi Penjualan Mobil Astra Isuzu. *Techno. Com*, 19(4), 364-374.
- [12] Wibawa, E. S., & Mustofa, Z. (2021). Implementasi Aplikasi Sistem Peramalan Persediaan Barang Menggunakan Metode Single Moving Average Berbasis Web. *Elkom: Jurnal Elektronika dan Komputer*, 14(2), 224-233.