JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

PENGAMANAN DOKUMEN KEPEGAWAIAN PADA DINAS PENDIDIKAN TEMANGGUNG DENGAN ALGORITMA RC4 DAN AES-256

Fathur Setya Pratama[1], Moh Ali Romli[2]

[1,2]Universitas Teknologi Yogyakarta, Sleman 55285
** Email Korespondensi: fathursetya11@gmail.com, ali.romli@uty.ac.id*

INFO ARTIKEL

Sejarah Artikel:
Diterima. Tgl 27/09/23
Diperbaiki Tgl 17/12/23
Disetujui. Tgl 26/12/23
Tersedia daring Tgl 03/01/2024

e-ISSN 2961-9009
p-ISSN 2963-1289

ABSTRAK

Dinas Pendidikan, Kepemudaan, dan Olahraga Kabupaten Temanggung adalah sebuah instansi pemerintahan yang bertanggung jawab atas sektor pendidikan, budaya, dan olahraga di Kabupaten Temanggung. Saat ini, dokumen-dokumen kepegawaian di lembaga ini masih tersimpan tanpa pembatasan akses tertentu. Kondisi seperti ini memberikan peluang bagi individu yang tidak berhak untuk mengakses dokumen kepegawaian tersebut. Kekurangan dalam perlindungan data berpotensi menimbulkan risiko kebocoran dan manipulasi data. Oleh karena itu, dilakukan penelitian yang melibatkan penggunaan metode kriptografi RC4 yang digabungkan dengan metode AES-256 untuk meningkatkan keamanan dokumen kepegawaian. Dokumen akan dienkripsi menggunakan metode RC4, di mana nilai-nilai akan mengalami permutasi sebelum dienkripsi lebih lanjut menggunakan metode AES-256. Proses enkripsi ini melibatkan empat jenis konversi byte, yaitu SubBytes, ShiftRows, MixColumns, dan AddROUNDKey. Hasil pengujian menunjukkan bahwa enkripsi yang diterapkan berhasil berfungsi dengan baik, sehingga individu yang tidak memiliki kunci enkripsi tidak dapat mengakses dokumen tersebut. Dengan demikian, keamanan dokumen kepegawaian dapat ditingkatkan, dan akses yang tidak sah dapat dicegah.

DOI :
https://doi.org/10.58290/jukomtek.v2i2.167

Kata Kunci:
Kriptografi, Enkripsi, Data, RC4, AES-256.

e-ISSN 2961-9009
p-ISSN 2963-1289

PENDAHULUAN

Kebocoran data yang sering terjadi dapat disebabkan oleh beragam faktor, termasuk kelalaian manusia, kelemahan dalam sistem, serta serangan siber yang dilakukan oleh pihak yang tidak bertanggung jawab. Selain itu, kekurangan dalam pengaturan akses juga menjadi pemicu utama terjadinya kebocoran data yang mudah terjadi. Apabila suatu dokumen tidak memiliki pembatasan akses yang sesuai, maka siapa pun dapat mengaksesnya tanpa perlu mendapatkan izin khusus, bahkan oleh pihak yang seharusnya tidak memiliki hak akses. Situasi semacam ini menghadirkan risiko yang signifikan, terutama ketika data yang terkandung dalam dokumen tersebut bersifat sensitif dan rahasia, sehingga rentan terhadap pencurian atau penyalahgunaan.

Dinas Pendidikan, Kepemudaan, dan Olahraga Kabupaten Temanggung berperan sebagai entitas pemerintahan yang memonitor dan mengelola data kepegawaian, termasuk para guru, kepala sekolah, staf sekolah, dan lainnya. Di dalam lembaga ini, terdapat permasalahan yang perlu diatasi, yaitu ketiadaan sistem keamanan untuk melindungi dokumen-dokumen kepegawaian. Akibatnya, dokumen-dokumen tersebut dapat diakses oleh siapapun, bahkan oleh pihak yang tidak memiliki kepentingan sah terhadap dokumen tersebut.

Situasi ini menunjukkan bahwa ada kelemahan dalam melindungi serta mengatur akses terhadap informasi yang bersifat rahasia dan pribadi. Sistem keamanan yang tidak memadai dapat membuka potensi risiko pencurian identitas, penyebaran informasi pribadi secara ilegal, atau penyalahgunaan data oleh pihak yang tidak memiliki izin. Sebagai akibatnya, perlindungan terhadap data kepegawaian menjadi masalah yang harus segera diatasi secara serius.

Penelitian ini akan menggunakan metode enkripsi yang melibatkan Algoritma *Rivest Code 4* (RC4) dan *Advanced Encryption Standard* (AES) dengan kunci berukuran 256 bit. Algoritma RC4 melakukan permutasi nilai selama proses enkripsi, dan kemudian nilai-nilai tersebut diacak menggunakan kunci yang telah ditentukan sebelumnya. Sementara itu, Algoritma *Advanced Encryption Standard* dengan kunci 256 bit (AES-256) melibatkan beberapa tahap perputaran dan konversi byte, termasuk *SubBytes, ShiftRows, MixColumns, dan AddROUNDKey.*

Ruang Lingkup atau batasan masalah dalam konteks penelitian ini mencakup beberapa aspek sebagai berikut:

a. Teknologi yang diterapkan dalam pembangunan sistem ini berbasis web.
b. Objek penelitian yang menjadi fokus adalah dokumen kepegawaian dalam format pdf, docx, dan xlsx yang tersedia di Dinas Pendidikan, Kepemudaan, dan Olahraga Kabupaten Temanggung.
c. Setelah proses enkripsi, format *file* yang disimpan dalam sistem adalah berekstensi txt.
d. Ukuran *file* dokumen yang digunakan dalam proses enkripsi tidak melebihi kapasitas sebesar 3MB.

Penelitian ini bertujuan untuk menerapkan algoritma kriptografi RC4 dan AES-256 dalam melindungi data yang terkandung dalam dokumen kepegawaian yang dimiliki oleh Dinas Pendidikan, Kepemudaan, dan Olahraga Kabupaten Temanggung.

LANDASAN TEORI

Dokumen

Dokumen adalah catatan sah yang digunakan sebagai bukti atau dukungan untuk pernyataan tertentu. Dalam konteks komputasi, dokumen merujuk pada *file* yang dihasilkan melalui perangkat lunak seperti Microsoft Word, Corel Draw, Notepad, dan berbagai aplikasi lainnya. Meskipun pada awalnya istilah "dokumen" terutama mengacu pada dokumen pengolah kata, sekarang ini mencakup berbagai jenis *file* yang dapat disimpan. Dengan demikian, dokumen dapat berisi teks, gambar, audio, video, serta berbagai jenis data lainnya. Setiap dokumen diidentifikasi dengan ikon dan memiliki nama *file* yang unik. (Tanjung, 2021).

File dokumen adalah kumpulan informasi khusus yang tersimpan dalam sistem berkas yang hanya dapat diakses oleh individu yang memiliki izin akses. Pemanfaatan *file* dokumen adalah sebagai sarana komunikasi yang memudahkan

e-ISSN 2961-9009
p-ISSN 2963-1289

penyampaian dan penyebaran informasi, baik dari individu kepada sekelompok orang yang lebih besar. Isi dari data atau informasi dalam *file* dokumen sering kali melibatkan materi yang memiliki nilai penting atau bahkan bersifat rahasia.(Marpaung, dkk., 2023).

Kepegawaian

Kepegawaian merupakan segala kegiatan yang berkaitan dengan kepentingan pekerjaan (Wijaya, dkk., 2022). Berdasarkan konsep tersebut, konsep kepegawaian mencakup seluruh aspek yang terkait dengan status, tugas, hak, dan perkembangan seorang pegawai. Oleh karena itu, dapat disimpulkan bahwa kepegawaian adalah bagian dari suatu entitas yang memiliki fokus utama pada sumber daya manusianya, termasuk segala hal yang berkaitan dengan tugas, posisi, hak, pengembangan, dan kompensasi dari sumber daya manusia tersebut, semuanya termasuk dalam ruang lingkup kepegawaian.

Data

Menurut Jogiyanto (2007), data adalah informasi yang dikumpulkan dari pengamatan, dapat berwujud angka, simbol, atau karakteristik. Data ini merupakan informasi dasar tentang manusia, lokasi, kejadian, dan hal-hal penting lainnya yang disusun dengan baik. Dalam konteks ini, data memiliki potensi untuk diubah menjadi informasi yang lebih bermanfaat dan signifikan bagi para penggunanya.

Sistem Keamanan Data

Saputro (2021), mengemukakan bahwa sebuah sistem adalah gabungan beberapa komponen yang saling terhubung untuk mencapai tujuan tertentu. Sistem itu sendiri memiliki elemen penggerak yang membantu setiap komponen mencapai tujuan mereka dalam hubungannya dengan komponen lain. Dalam sistem terdapat sekelompok komponen yang berinteraksi satu sama lain untuk mencapai suatu tujuan. Sebagian besar sistem terdiri dari subsistem yang lebih kecil yang berperan dalam mendukung sistem yang lebih besar.

Kriptografi

Jamaludin, dkk. (2022), kriptografi merupakan ilmu yang mempelajari metode matematis yang berkaitan dengan aspek keamanan informasi seperti menjaga kerahasiaan, integritas data, dan melakukan otentikasi. Kriptografi, pada dasarnya, terdiri dari dua tahap utama, yaitu enkripsi dan dekripsi. Tahap enkripsi adalah proses mengubah pesan terbuka (*plaintext*) menjadi pesan rahasia (*chipertext*), yang kemudian dikirim melalui saluran komunikasi terbuka. Ketika pesan yang sudah dienkripsi ini diterima oleh penerima, pesan tersebut akan didekripsi kembali menjadi pesan terbuka (*plaintext*) dalam proses yang sering disebut dekripsi. Hal ini memungkinkan pesan dapat diterima dan dibaca oleh penerima pesan. Enkripsi adalah cara untuk mengubah pesan atau data menjadi teks yang tidak dapat dibaca.

Setyawati, dkk. (2021), kriptografi merupakan langkah yang rasional untuk menyembunyikan pesan dari pihak yang tidak memiliki izin untuk menerima pesan tersebut. Oleh karena itu, kriptografi mewakili studi tentang keamanan informasi, yang mencakup prinsip-prinsip keamanan data seperti menjaga kerahasiaan, integritas, dan otentikasi informasi sehingga tidak sembarang individu dapat mengaksesnya. Beberapa jenis kriptografi yang ada termasuk kriptografi dengan kunci simetris dan kriptografi dengan kunci asimetris.

Rivest Code 4

Menurut Haris, dkk. (2020), *Rivest Code 4* (RC4) merupakan metode enkripsi yang memiliki tingkat kecepatan yang lebih tinggi dibandingkan dengan berbagai metode enkripsi lainnya seperti Data Encryption Standard (DES), Triple DES, Blowfish 256, serta *Advanced Encryption Standard* (AES) tipe 128 dan AES-256. Algoritma ini sering digunakan dalam berbagai sistem keamanan, termasuk dalam protokol *Secure Socket Layer* (SSL). Keunggulan dari algoritma enkripsi ini terletak pada kesederhanaannya, sehingga memudahkan dalam proses implementasinya. Ron Rivest dari laboratorium RSA adalah pencipta algoritma RC4. Dalam kriptosistem RC4, terdapat sebuah ruang yang berupa tabel permutasi 256 bit yang kemudian diacak dengan menggunakan kunci. Sebelum proses enkripsi dan dekripsi dalam sistem kriptografi RC4, sistem sandi RC4 akan melakukan

e-ISSN 2961-9009
p-ISSN 2963-1289

inisialisasi terhadap statusnya menggunakan sebuah algoritma yang dikenal dengan istilah "penjadwalan kunci.".

RC4 adalah tipe algoritma aliran yang berarti setiap operasi enkripsi dilakukan pada satu bit karakter per kali prosesnya. Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu jenis algoritma kunci simetris yang dikembangkan oleh RSA Data Security Inc (RSADSI) dalam bentuk stream cipher. Algoritma RC4 memungkinkan penggunaan panjang kunci yang bervariasi, mulai dari 1 hingga 256 bit, yang kemudian digunakan untuk menginisialisasi tabel berukuran 256 bit. (Umar & Soetanto, 2022).

Advanced Encryption Standard (AES)

Algoritma *Advanced Encryption Standard* (AES) adalah algoritma enkripsi yang termasuk dalam kategori tipe terenkripsi blok, serta merupakan salah satu jenis algoritma kunci simetris yang mengadopsi penggunaan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi. Enkripsi dalam AES dilakukan melalui serangkaian proses yang berulang yang dikenal dengan istilah "putaran." Jumlah putaran yang dilakukan dalam algoritma AES bergantung pada panjang kunci yang digunakan dalam proses tersebut. Setiap putaran memerlukan kunci putaran serta hasil dari putaran sebelumnya. Berdasarkan panjang kunci yang digunakan, yaitu kunci ronde yang dihasilkan, enkripsi dan dekripsi data dalam algoritma AES dapat dilakukan dengan menggunakan kunci berukuran 128 bit, 192 bit, atau 256 bit. (Nurhareza & Siswanto, 2022).

Teknologi Web

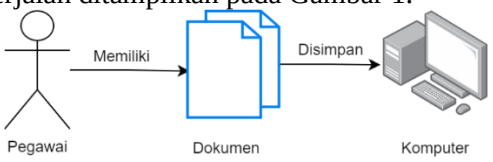
Web merupakan sebuah aplikasi yang memuat beragam dokumen multimedia, seperti teks, gambar, animasi, dan video. Akses terhadap web dilakukan melalui protokol *Hypertext Transfer Protocol* (HTTP) dengan menggunakan perangkat lunak yang dikenal sebagai *browser*. (Oktaviani & Ayu, 2021).

Flowchart

Flowchart atau bagan alir adalah representasi grafis yang secara logis memandu aliran dari suatu proses atau program dalam suatu sistem. *flowchart* digunakan sebagai cara untuk menggambarkan langkah-langkah yang terlibat dalam menyelesaikan masalah dengan menggunakan simbol-simbol yang mudah dimengerti, *user-friendly*, dan mengikuti format standar (Syamsiah, 2019). Penggunaan flowchart bertujuan untuk mengilustrasikan langkah-langkah penyelesaian suatu masalah dengan cara yang sederhana, jelas, dan terstruktur, dengan memanfaatkan simbol-simbol standar yang dapat dimengerti oleh seorang *programmer*.

METODOLOGI PENELITIAN

Saat ini, sistem yang digunakan di lembaga terkait belum memadai dalam aspek keamanan data dokumen. Dalam proses pengolahan, penyaluran, dan penyimpanan dokumen kepegawaian, belum ada penerapan sistem keamanan data yang efektif. Data hanya disimpan pada komputer atau hardisk kantor tanpa adanya lapisan perlindungan yang memadai. Demikian pula, dalam proses penyaluran data melalui *email*, *hardisk*, *flashdisk*, CD, DVD, maupun sistem yang sudah ada, tidak ada tindakan pengamanan data yang diterapkan.. Alur sistem yang berjalan ditampilkan pada Gambar 1.



Gambar 1 Alur Sistem Saat Ini

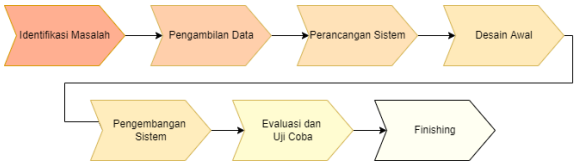
Berdasarkan Gambar 1, dokumen yang dikelola di lembaga tersebut, baik yang disimpan secara daring maupun luring, seperti dokumen dengan format docx, xlsx, dan pdf, memiliki potensi risiko kebocoran data karena dapat diakses oleh individu yang tidak memiliki izin akses pada dokumen tersebut. Dampak dari kebocoran data ini dapat berdampak negatif pada lembaga dan masyarakat secara keseluruhan. Oleh karena itu, perlu segera diterapkan sistem keamanan modern yang lebih efektif guna mengurangi potensi risiko yang ada.

Tahapan Penelitian

Penelitian ini mencakup sejumlah langkah penelitian yang akan ditempuh oleh

e-ISSN 2961-9009
p-ISSN 2963-1289

peneliti. Langkah-langkah penelitian dilakukan secara terstruktur dengan tujuan agar penelitian ini dapat diselesaikan sesuai jadwal yang telah ditentukan. Rincian mengenai langkah-langkah penelitian dapat ditemukan dalam Gambar 2.

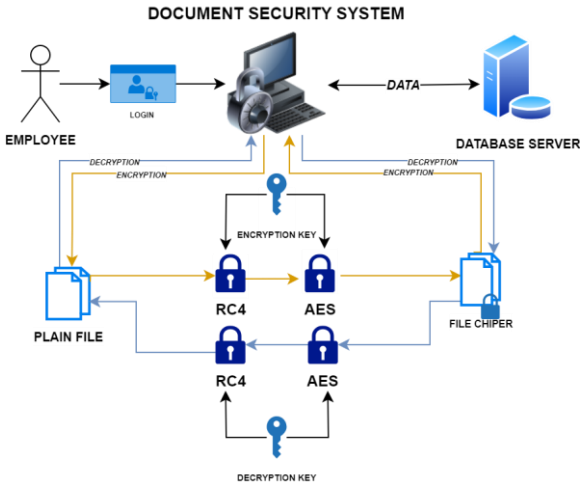


Gambar 2 Tahapan Penelitian

Berdasarkan Gambar 2, terdapat penjelasan mengenai serangkaian langkah penelitian yang ditempuh oleh peneliti. Langkah-langkah tersebut meliputi identifikasi permasalahan, pengumpulan data, perancangan sistem, pembuatan desain awal, pengembangan sistem, evaluasi dan uji coba, serta tahap penyelesaian (*finishing*).

Penelitian yang Dilakukan

Sistem yang dibangun adalah sistem keamanan dokumen kepegawaian dengan metode kriptografi AES-256 dan RC4. Sistem yang diusulkan terdapat pada Gambar 3.



Gambar 3 Sistem yang Diusulkan

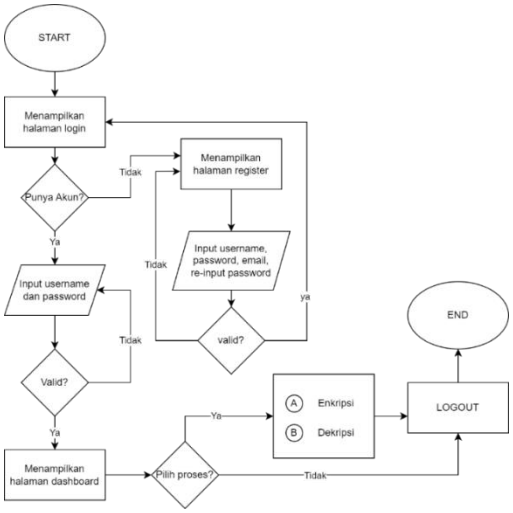
Berdasarkan Gambar 3, model dari sistem yang dibangun dapat secara umum dibagi menjadi dua tahap utama, yaitu tahap enkripsi dan tahap dekripsi. Pada tahap enkripsi, pengguna memasukkan dokumen ke dalam sistem, dan sistem kemudian melakukan proses enkripsi dengan menggunakan kunci yang telah dimasukkan oleh pengguna. Proses enkripsi ini melibatkan dua metode, yakni enkripsi dengan metode RC4 diikuti oleh enkripsi dengan metode AES-256. Setelah proses enkripsi selesai, hasilnya berupa *chiperfile* (*file* terenkripsi) yang dapat disimpan dalam database sistem atau diunduh dan bahkan dihapus oleh pengguna.

Tahap kedua adalah tahap dekripsi, di mana chiper*file* hasil enkripsi sebelumnya dimasukkan ke dalam sistem dan kemudian didekripsi menggunakan dua metode, yaitu dengan metode AES-256 diikuti oleh metode RC4. Kunci yang digunakan dalam tahap dekripsi ini adalah kunci yang sama dengan yang digunakan dalam proses enkripsi. Ini disebabkan oleh fakta bahwa algoritma kriptografi RC4 dan AES adalah jenis kriptografi simetris, yang berarti mereka hanya memerlukan satu kunci. Setelah proses dekripsi selesai, dokumen yang awalnya telah dienkripsi kembali menjadi dokumen aslinya. File dokumen yang telah didekripsi disimpan dalam *database server*, dan dokumen ini dapat dikelola oleh pengguna melalui fungsi manajemen *file*.

Flowchart Login

Dalam penelitian ini, digunakan *Flowchart Diagram* sebagai alat untuk mengilustrasikan desain sistem yang dibangun. *Flowchart Diagram* digunakan untuk menggambarkan cara sistem beroperasi, termasuk tahapan proses *login*, pendaftaran, dan akses pengguna ke dalam sistem. *Flowchart* merupakan representasi visual dari urutan langkah-langkah dalam suatu sistem. Dalam konteks ini, flowchart digunakan untuk memvisualisasikan langkah-langkah yang terlibat dalam proses *login* dan pendaftaran pengguna, serta bagaimana pengguna dapat mengakses sistem setelah berhasil melakukan *login* atau pendaftaran. Gambaran detail dari *flowchart* terdapat pada Gambar 4.

e-ISSN 2961-9009
p-ISSN 2963-1289

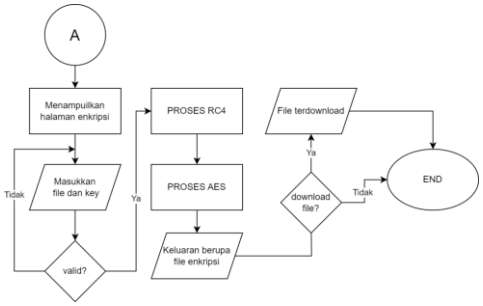


Gambar 4 *Flowchart* Login

Berdasarkan gambar Gambar 4, pengguna yang ingin mengakses sistem akan melewati tahap *login* sebagai langkah awal. Jika pengguna belum memiliki akun, mereka akan diarahkan ke halaman pendaftaran. Pada halaman pendaftaran, pengguna diminta untuk mengisi informasi seperti *username, password,* alamat email, dan mengulangi penulisan *password*. Validitas data yang dimasukkan pengguna akan diuji, dan jika tidak valid, pengguna tidak dapat melanjutkan proses pendaftaran. Namun, jika pengguna memasukkan informasi dengan benar, mereka akan diarahkan kembali ke halaman *login* untuk menginputkan *username* dan *password* yang telah didaftarkan sebelumnya. Apabila pengguna berhasil memasukkan *username* dan *password* dengan benar pada tahap *login*, mereka akan diarahkan ke halaman utama (*dashboard*) sistem.

Flowchart Enkripsi Data

Flowchart enkripsi menggambarkan proses yang terjadi pada halaman enkripsi. Pada bagian ini, *flowchart* menggambarkan langkah-langkah yang terlibat pada halaman enkrpsi data. Proses enkripsi terdapat pada Gambar 5.

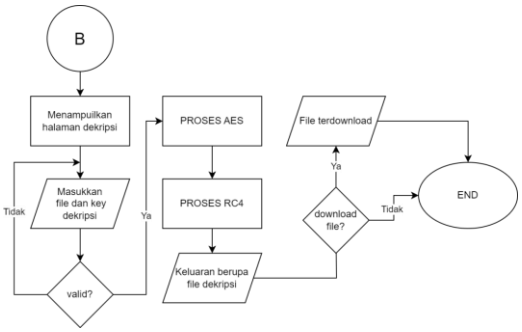


Gambar 5 Enkripsi

Bagian halaman enkripsi data, pengguna yang telah berhasil *login* memiliki kemampuan untuk melakukan proses enkripsi data. Proses ini melibatkan penggunaan *file* yang akan dienkripsi dan kunci yang digunakan. Jika *file* dan kunci yang dimasukkan valid, sistem akan menjalankan proses enkripsi menggunakan algoritma RC4 dan AES. Hasil dari proses enkripsi ini adalah *file* chiper yang nantinya dapat diunduh oleh pengguna.

***Flowchart* Dekripsi Data**

Flowchart dekripsi menggambarkan proses yang terjadi pada halaman enkripsi. Proses enkripsi terdapat pada Gambar 6.



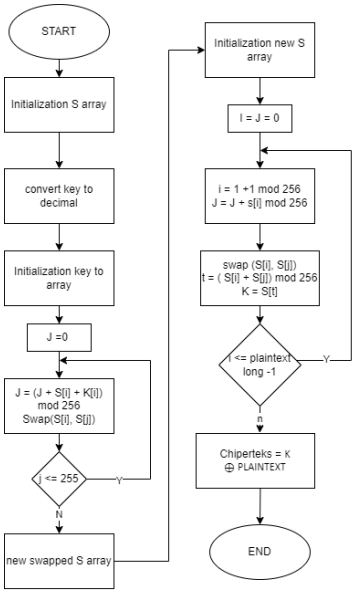
Gambar 6 *Flowchart* Dekripsi

Bagian halaman dekripsi data, pengguna yang telah *login* memiliki kemampuan untuk menjalankan proses dekripsi data. Untuk melakukan dekripsi, pengguna perlu memasukkan *file* enkripsi dan kunci yang sesuai. Jika *file* enkripsi dan kunci yang dimasukkan valid, sistem akan melaksanakan proses dekripsi menggunakan algoritma AES dan RC4. Hasil dari proses dekripsi ini adalah *plain file* (*file* dalam bentuk teks biasa) yang dapat diunduh oleh pengguna.

***Flowchart* Algoritma Rivest Code 4**

e-ISSN 2961-9009
p-ISSN 2963-1289

Proses yang terjadi saat terjadinya enkripsi pada algoritma RC4 dapat dilihat pada Gambar 7.

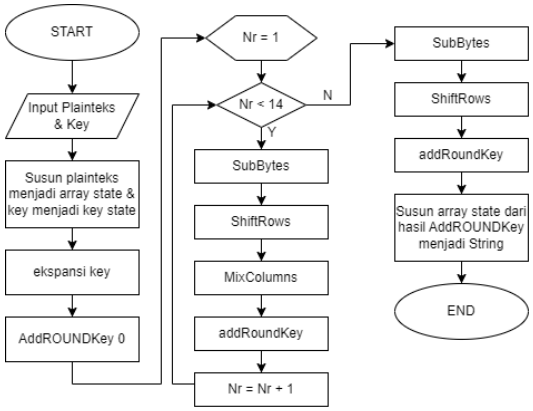


Gambar 7 *Flowchart* RC4

Berdasarkan Gambar 7, dapat dijelaskan bahwa Algoritma RC4 memiliki dua tahap utama, yakni tahap *Key Stream Array* dan tahap *Pseudo-Random Generation Automation*. Tahap *Key Stream Array* digambarkan pada sisi kiri dari *flowchart*, sementara *Pseudo-Random Generation Automation* digambarkan pada sisi kanan dari *flowchart*. Dalam kedua tahap tersebut, terdapat beberapa kali proses *swap array* yang dilakukan, dengan setidaknya satu kali swap yang mengubah *array* S dan digunakan sebagai pembangkit kunci atau *keystream*. Setelah berhasil dibangkitkan, kunci tersebut kemudian digunakan untuk menghasilkan *chipertext* dengan melakukan operasi exclusive or (xor) antara *keystream* dan *plaintext*.

Flowchart Advenced Encryption Standard

Proses yang terjadi saat dilakukanya enkripsi dengan Algoritma *Advenced Encryption Standard* (AES) dapat dilihat pada Gambar 8.



Gambar 8 *Flowchart* AES

Berdasarkan Gambar 8 dapat dijelaskan bahwa Algoritma AES melibatkan beberapa tahap dalam prosesnya, seperti *AddRoundKey, SubBytes, ShiftRows, dan MixColumns*. Proses-proses ini diulang sebanyak 13 kali putaran karena dalam kasus ini digunakan AES tipe 256. *AddRoundKey* awal digunakan sebagai operasi xor untuk menentukan langkah-langkah selanjutnya, sementara *AddRoundKey* pada putaran terakhir adalah *chipertext* itu sendiri. Namun, perlu diingat bahwa diagram pada Gambar 8 hanya merupakan representasi singkat dari proses yang terjadi dalam Algoritma AES. Pada implementasi yang sebenarnya, terdapat tahapan yang lebih panjang dan sangat kompleks.

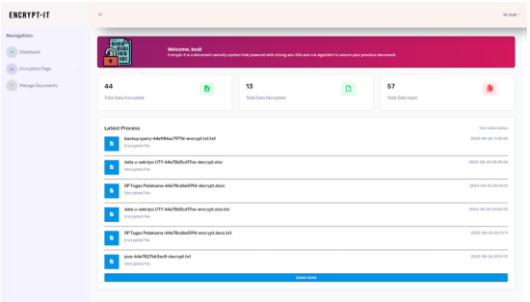
HASIL DAN PEMBAHASAN

Implementasi pada penelitian ini menjelaskan penerapan sistem dari rancangan yang telah dibuat sebelumnya menjadi kode aplikasi web yang dapat dijalankan.

Implementasi *Dashboard*

Halaman *dashboard* adalah halaman pertama yang muncul ketika pengguna berhasil *login* ke dalam sistem. Pada halaman ini, terdapat informasi mengenai statistik sistem, seperti jumlah data yang telah dimasukkan, jumlah data yang telah dienkripsi, dan jumlah data yang telah didekripsi. Halaman *dashboard* terdapat pada Gambar 9.

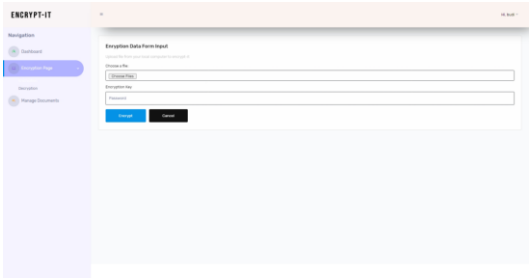
e-ISSN 2961-9009
p-ISSN 2963-1289



Gambar 9 Tampilan *Dashboard*

Implementasi Halaman Enkripsi

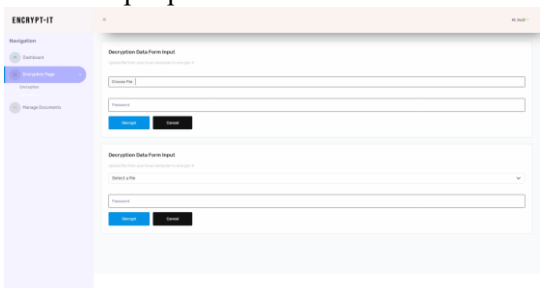
Halaman enkripsi data merupakan halaman di mana pengguna dapat mengunggah data yang ingin dienkripsi menggunakan sistem ini. Di halaman ini, terdapat dua bidang yang berisi input *file* dan input kunci enkripsi. Setelah pengguna mengisi kedua bidang tersebut, mereka dapat mengeksekusi proses enkripsi data dengan menekan tombol "enkripsi data." Jika proses enkripsi berhasil, pengguna akan menerima notifikasi keberhasilan. Halaman Enkripsi Data terdapat pada Gambar 10.



Gambar 10 Tampilan Halaman Enkripsi

Implementasi Halaman Dekripsi

Halaman dekripsi data adalah halaman di mana pengguna dapat mengunggah atau memilih data yang akan didekripsi menggunakan sistem ini. Di halaman ini, terdapat dua formulir, di mana satu formulir digunakan untuk melakukan dekripsi pada *file* yang terdapat di perangkat pengguna, sementara formulir lainnya digunakan untuk dekripsi *file* yang sudah ada dalam sistem. Pada setiap formulir terdapat dua bidang, di mana satu bidang digunakan untuk memilih *file* yang akan didekripsi, dan bidang lainnya digunakan untuk memasukkan kunci dekripsi. Setelah pengguna mengisi kedua bidang tersebut, mereka dapat memulai proses dekripsi data dengan mengeksekusi tombol "dekripsi data". Halaman Dekripsi Data terdapat pada Gambar 11.



Gambar 11 Tampilan Halaman Dekripsi

Hasil

Hasil yang diharapkan dari *file* yang telah mengalami proses enkripsi adalah sebuah *chipertext* yang tidak dapat dibaca seperti *file* aslinya. Dalam sistem ini, semua *file* yang dienkripsi akan menghasilkan chiper*file* dengan format txt. Berikut ini ditunjukkan perbandingan antara *file* sebelum dan sesudah proses enkripsi.

PEMERINTAH KABUPATEN TEMANGGUNG
DINAS PENDIDIKAN, KEPEMUDAAN DAN OLAH RAGA

SURAT PERINTAH
Nomor : 821.4/ /V/2022

DASAR : Kepentingan Dinas;

MEMERINTAHKAN

KEPADA : Nama : SEPTI WIJAYANTI
NIP : 19810816201406200l
Pangkat, Gol/Ruang : Pengatur Muda Tk. I, II/b
Jabatan : Pengelola Kurikulum Peningkatan Mutu Sekolah

UNTUK : Melaksanakan tugas sebagai Pengelola Pengendalian Masyarakat, Seksi Pendidikan Masyarakat, Bidang Pembinaan Pendidikan Non Formal Dinas Pendidikan, Kepemudaan dan Olah Raga Kabupaten Temanggung.

KETERANGAN : 1. Surat Perintah ini berlaku mulai tanggal ditetapkan ;
2. Surat Perintah ini agar dilaksanakan dengan penuh tanggung jawab ;
3. Apabila ada kekeliruan dalam Surat Perintah ini akan diadakan perbaikan sebagaimana mestinya.

Gambar 12 *file* Sebelum Proses Enkripsi

Gambar 13 Hasil Enkripsi *file* Docx

e-ISSN 2961-9009
p-ISSN 2963-1289

PENUTUP

Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa metode kriptografi RC4 dan AES-256 telah berhasil diterapkan untuk meningkatkan keamanan dokumen kepegawaian di Dinas Pendidikan, Kepemudaan, dan Olahraga Kabupaten Temanggung. Hasil penelitian menunjukkan bahwa penggunaan metode ini efektif dalam meningkatkan keamanan dokumen, mengurangi risiko akses yang tidak sah, dan mengurangi potensi pelanggaran data. Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam bidang keamanan informasi dan menyediakan solusi yang dapat diadopsi oleh lembaga serupa untuk mengamankan data-data penting mereka.

ACKNOWLEDGEMENTS

Paper ini adalah hasil penelitian Tugas Akhir Mahasiswa.

DAFTAR PUSTAKA

Awaludin Umar, R., & Soetanto, H. (2022). Implementasi Algoritma RC4 Untuk Keamanan *file* Berbasis Web Pada SD IT Ar Rahman. In *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*. https://senafti.budiluhur.ac.id/index.php/senafti/article/view/442/26

Haris, M., Nugroho, N. B., & Ginting, R. I. (2020). Implementasi Keamanan Data Gaji Pada Dinas Komunikasi Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4. *Seminar Nasional Riset Dan Inovasi Teknologi*, *5*, 803–808. https://ojs.trigunadharma.ac.id/

Jogiyanto, H. M. (2007). Sistem informasi keperilakuan. Yogyakarta: Andi Offset, 235.

Marpaung, A., Ramadhan, P. S., & Pranata, A. (2023). Implementasi RSA Untuk Enkripsi Dan Dekripsi *file* Dokumen. *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, *2*(1), 39. https://doi.org/10.53513/jursi.v2i1.532

Nurhareza, I. K., & Siswanto, S. (2022). Penerapan Algoritma Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Keluharan Belendung. In *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*. https://senafti.budiluhur.ac.id/index.php/senafti/article/view/269/35

Oktaviani L, & Ayu M. (2021). Pengembangan Sistem Informasi Sekolah Berbasis Web Dua Bahasa SMA Muhammadiyah Gading Rejo. *Jurnal Pengabdian Pada Masyarakat*, *6*(2), 437–444. https://doi.org/https://doi.org/10.30653/002.202162.731

Saputro, A. C. (2021). Perancangan Aplikasi Penyewaan Mobil Berbasis Android Pada CV GAP Transport. *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer Dan Aplikasinya*, 1–6. https://conference.upnvj.ac.id/index.php/senamika/article/view/1358/1063

Setyawati, E., Widjayanti, C. E., Siraiz, R. R., & Wijoyo, H. (2021). Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5. *Jurnal Manajamen Informatika Jayakarta*, *1*(1), 56. https://doi.org/10.52362/jmijayakarta.v1i1.367

Syamsiah, S. (2019). Perancangan Flowchart dan Pseudocode Pembelajaran Mengenal Angka dengan Animasi untuk Anak PAUD Rambutan. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *4*(1), 86. https://doi.org/10.30998/string.v4i1.3623

Tanjung, R. Y. (2021). Perancangan Aplikasi Kompresi *file* Dokumen Menggunakan Algoritma Adiitive Code. *Jurnal Riset Komputer)*, *8*(4), 2407–389. https://doi.org/10.30865/jurikom.v8i4.3593

Wijaya, A., Hendrastuty, N., & Ghufroni An, M. (2022). Rancang Bangun Sistem Informasi Manajemen Kepegawian (SIMPEG) Berbasis Web (Studi Kasus: PT Sembilan Hakim Nusantara). *Jurnal*

e-ISSN 2961-9009
p-ISSN 2963-1289

Teknologi Dan Sistem Informasi (JTSI), *3*(1), 77. http://jim.teknokrat.ac.id/index.php/JTSI