SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

APLIKASI PENGAMANAN *FILE* DOKUMEN MENGGUNAKAN ALGORITMA AES-128 DAN RC4 PADA SEKOLAH SMK YADIKA 3

Rezki Naenro Lubis[1*], Utomo Budiyanto[2]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]naenrolubis@gmail.com, [2]utomo.budiyanto@budiluhur.ac.id
(* : corresponding author)

Abstrak- SMK Yadika 3 merupakan sebuah sekolah swasta di Jakarta Barat yang memiliki tiga program keahlian Teknik Jaringan Komputer, Teknik Kendaraan Ringan, Teknik Bisnis Sepeda Motor. SMK Yadika 3 memiliki berbagai dokumen penting seperti data siswa, data guru, dan soal ujian yang disimpan di dalam folder penyimpanan komputer. Saat ini, sekolah ini belum memiliki sistem pengamanan khusus, yang membuat dokumen-dokumen tersebut rentan terhadap akses oleh pihak yang tidak berkepntingan. Penelitian ini bertujuan untuk membuat aplikasi pengamanan *file* berbasis web guna melindungi dokumen-dokumen penting dari akses tidak sah. Untuk mencapai tujuan ini, aplikasi menggunakan teknik kriptografi yang menggabungkan algoritma *Advanced Encryption Standard* (AES-128) dan *Rivest Code 4* (RC4), di mana proses enkripsi melibatkan AES-128 diikuti oleh RC4, dan dekripsi menggunakan RC4 diikuti oleh AES-128. Aplikasi ini dibuat menggunakan bahasa pemrograman PHP. Hasil penelitian menunjukkan bahwa aplikasi yang dikembangkan berhasil mengenkripsi dan mendekripsi dokumen dengan mengubahnya menjadi matriks *hexadecimal* 4 x 4, yang dikenal sebagai state, sehingga memastikan keamanan data. Hanya *individu* yang mengetahui *password* yang dapat mengakses dokumen tersebut dan mengembalikan dokumen seperti semula. Penelitian ini memberikan solusi praktis untuk pengamanan dokumen penting di lingkungan pendidikan dengan menggunakan kombinasi algoritma AES-128 dan RC4. Aplikasi yang dibuat dapat meningkatkan keamanan data sekolah dan mencegah akses tidak sah, yang memberikan kontribusi penting bagi pengelolaan informasi dan data di SMK Yadika 3.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, AES-128, RC4.

DOCUMENT FILE SECURITY APPLICATION USING AES-128 AND RC4 ALGORITHMS AT YADIKA 3 VOCATIONAL SCHOOL

Abstract- *SMK Yadika 3 is a private school in West Jakarta with three specialized programs: Computer Network Engineering, Light Vehicle Engineering, and Motorcycle Business Engineering. The school maintains various important documents, such as student data, teacher data, and exam questions, stored in a computer storage folder. Currently, the school lacks a dedicated security system, making these documents vulnerable to unauthorized access. This study aims to develop a web-based file security application to protect these important documents from unauthorized access. To achieve this goal, the application utilizes a cryptographic technique that combines the Advanced Encryption Standard (AES-128) and Rivest Code 4 (RC4) algorithms, where the encryption process involves AES-128 followed by RC4, and decryption uses RC4 followed by AES-128. The application is developed using the PHP programming language. The results of the study demonstrate that the developed application successfully encrypts and decrypts documents by converting them into a 4 x 4 hexadecimal matrix, known as a state, thereby ensuring data security. Only individuals who know the password can access the documents and restore them to their original state. This study provides a practical solution for securing important documents in educational settings using a combination of AES-128 and RC4 algorithms. The application enhances school data security and prevents unauthorized access, making a significant contribution to information and data management at SMK Yadika 3.*

Keywords*: Cryptography, Encryption, Decryption, AES-128, RC4.*

1. PENDAHULUAN

Arsip *file* berkas biasanya berisi laporan dan hasil pekerjaan. Pada sekolah terdapat dokumen penting seperti data siswa, data guru, soal ujian sekolah serta dokumen lain yang disimpan dalam folder penyimpanan di komputer sekolah. *File* berkas lainnya yang dianggap penting oleh sekolah harus dijaga keamanan dan kerahasiaannya [1]. Sekolah Menengah Kejuruan (SMK) Yadika 3 Tegal Alur didirikan oleh Yayasan Abdi Karya pada tahun 1990 dipimpin oleh bapak L.Ritonga S.kom. Sekolah ini berlamat di Jl. Kamal Raya No.42, RT.1/RW.6, Cengkareng Barat Kecamatan Cengkareng, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11730, SMK Yadika 3 adalah sekolah menengah kejuruan yang memiliki 3 jurusan didalamnya yaitu Teknik Jaringan Komputer, Teknik Kendaraan Ringan, dan Teknik Bisnis Sepeda Motor. SMK Yadika 3 memiliki berbagai *file* dokumen yang bersifat

penting seperti data guru, data siswa, dan soal ujian akhir semester. Dan dokumen penting lainnya yang tidak boleh diketahui oleh pihak yang tidak berkepentingan. Pada saat ini sekolah SMK Yadika 3 belum memiliki sistem pengamanan *file*, dan media penyimpanan seperti *database* yang berfungsi untuk menyimpan *file* dokumen. Sehingga ketika guru membutuhkan *file* yang diinginkan harus meminta *file* dari guru lain yang memiliki *file* tersebut, kegiatan ini dapat mengakibatkan kebocoran data, namun cara ini tidak menjamin keamanannya, untuk menjaga keamanan *file* dokumen penting diperlukan keamanan yang lebih kuat [2].

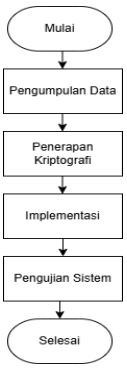
Berdasarkan latar belakang tersebut, terdapat sebagian metode guna melindungi *file* dokumen atau berkas di sekolah SMK Yadika 3 adalah dengan menggunakan aplikasi pengamanan *file* dokumen berbasis web yang memanfaatkan teknik kriptografi. Kriptografi adalah ilmu yang bertujuan melindungi kerahasiaan pesan dengan mengubahnya menjadi bentuk yang tidak dapat dipahami [3]. Cryptography berasal dari bahasa Yunani, terdiri dari dua kata, "*cryptos*" yang berarti "rahasia" serta "*graphia*" yang mengartikan "tulisan" [4]. Kriptografi bisa didefinisikan sebagai ilmu yang bertujuan melindungi informasi dan data dengan menggunakan cara dan pendekatan yang meliputi Kerahasiaan (*Confidentiality*), *Integritas*, serta Autentikasi (*Authentication*). [5]. Maksud dan tujuan dalam ilmu teknik penyandian, yang juga merupakan aspek keamanan informasi, meliputi Kerahasiaan (*Confidentiality*), Integritas Data (*Data Integrity*), Autentikasi (*Authentication*), dan Penyangkalan (*Non-repudiation*) [6].

Menurut penelitian sebelumnya yang dilakukan oleh (Rusyandi & Pradana) membahas, *Advanced Encryption Standard* AES dikenal sebagai algoritma dengan tingkat keamanan yang sangat tinggi. AES memiliki panjang kunci 128 bit dan dapat AES dapat bertahan dari serangan *exhaustive key search* [7]. Menurut penelitian sebelumnya yang dilakukan oleh (Umar & Hari) membahas, *Rivest Code 4* (RC4) merupakan algoritma sandi aliran yang enkripsi dan dekripsinya dilakukan setiap byte secara individual. Algoritma RC4 menggunakan kunci simetris (kunci yang sama) untuk enkripsi dan dekripsi data. RC4 dikenal karena kecepatan dan kesederhanaanya [8]. Maka dari itu, dalam penelitian kali ini membuat aplikasi pengamanan *file* dokumen berbasis web menggunakan metode *Advanced Encryption Standard* AES-128 dan *Rivest Code 4* (RC4). Proses pengubahan teks asli (*plaintext*) menjadi teks sandi (*ciphertext*) disebut enkripsi. Pesan yang sulit dibaca dinamakan *ciphertext*. Proses kebalikan dari enkripsi dinamakan dekripsi. Dekripsi mengembalikan teks sandi (*ciphertext*) sebagai teks asli (*plaintext*) [9].

Menurut penelitian sebelumnya maka tujuan dari penelitian ini membuat aplikasi untuk mengamankan *file* dokumen berbasis web yang dapat mengamankan *file* dokumen atau berkas penting pada sekolah SMK Yadika 3 dengan menggunakan metode kriptografi AES-128 dan RC4 agar file dokumen SMK Yadika 3 terlindungi dari individu yang tidak berkepentingan.

2. METODE PENELITIAN

Pada tahap ini, dijelaskan proses metode penelitian yang di mulai dari pengumpulan data hingga pengujian sistem pada Gambar 1.



Gambar 1. Metode Penelitian

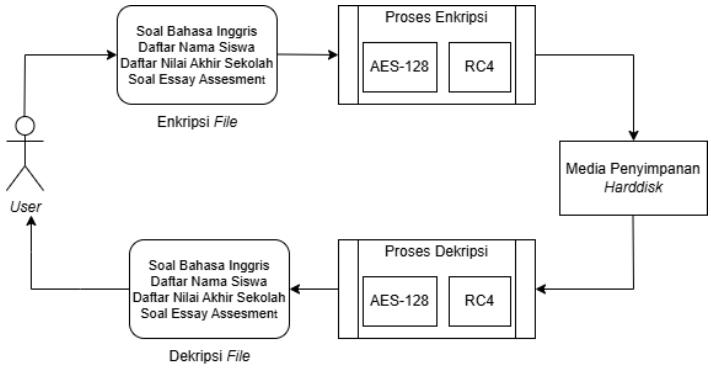
2.1. Pengumpulan Data

Pada tahap ini, melibatkan pengambilan informasi serta data terkait masalah di sekolah. Data dan informasi tersebut dikumpulkan melalui wawancara dan pengamatan. Proses wawancara dilakukan dengan cara mengajukan pertanyaan kepada individu disekolah yang ingin diwawancarai mengenai pengamanan *file*, khususnya kepada kepala sekolah SMK Yadika 3, untuk mengetahui apakah sekolah tersebut sudah memiliki sistem pengamanan *file*

atau belum. Selain itu, pengamatan dilakukan dengan datang langsung ke sekolah untuk mengetahui lebih lanjut prosedur sistem keamanan *file* yang bakal diterapkan pada sekolah SMK Yadika 3.

2.2. Penerapan Kriptografi

Pada tahap ini, menjelaskan proses enkripsi *file* dan dekripsi *file* [10]. Dimana *user* saat memilih *file* yang ingin dienkripsi akan masuk ke dalam proses enkripsi AES-128 terlebih dahulu. Selanjutnya dalam proses enkripsi AES-128 masuk ke tahapan pertama yaitu *Sub Bytes* merupakan proses mengganti *byte* menggunakan tabel *substitusi* (*S-box*), *Shift Rows* merupakan proses Menggeser baris-baris *array state* dengan cara (*wrapping*). *Mix Column* merupakan proses mengacak isi data disetiap kolom *array state*. *Add Round Key* proses melakukan operasi *XOR* pada *state* sekarang dengan *round key*. Selanjutnya adalah proses RC4 dimana dilakukan *inisialisasi S-Box* dan kunci rahasia, tahapan berikutnya dilakukan proses permutasian pada tabel *S-Box* dan *Random Key* hasil tersebut di *XOR* kan dengan *ciphertext* dari tahapan sebelumnya. Hasil dari *ciphertext* ini disimpan dalam *database*. Selanjutnya pada saat proses dekripsi *file* yang tersimpan dalam *database* diproses kembali menggunakan proses RC4 dan tahapannya sama yaitu *inisialisasi S-Box* dan *secret key* dilanjut dengan tahapan permutasian untuk *S-Box* dan pembangkitan *random key* dimana hasil tahapan tersebut di *XOR* kan dengan *ciphertext*. Dilanjut dengan proses AES-128 yang diproses ke dalam *Sub Bytes*, *Shift Rows*, *Mix Column* lalu *Add Round Key*, hasilnya di *XOR* kan dengan *ciphertext* yang dihasilkan RC4, lalu hasilnya ditampilkan kepada *user*. Oleh karena itu dengan permasalahan yang sudah dijelaskan, perlu sebuah aplikasi pengamanan *file* berbasis web guna mengamankan dokumen penting. Lalu pada aplikasi yang dibuat ini dapat merubah isi *file* aslinya menjadi data yang acak atau sulit dibaca, maka dari itu dokumen *file* yang bersifat rahasia dapat terlindungi. Untuk penjelasan lebih rinci dapat dilihat pada Gambar 2.



Gambar 2. Proses Enkripsi *File* dan Dekripsi *File*

2.3. Implementasi

Pada tahap ini, dilakukan perancangan menggunakan bahasa pemrograman tertentu. Berikut ini adalah aplikasi dan perangkat yang digunakan untuk proses tersebut:

a. *Software* yang dipakai untuk melindungi *file* dokumen menggunakan *Visual Studio Code*, yang memanfaatkan bahasa pemrograman *Hypertext Preprocessor* (PHP), sementara untuk basis data digunakan *MySQL*.
b. Perangkat keras yang mana digunakan meliputi prosesor *Intel Core i5-1135G7*, RAM berkapasitas 8GB, dan penyimpanan SSD dengan kapasitas 512GB.

2.4. Pengujian Sistem

Pada tahap ini, sistem yang segera dibuat dites untuk memastikan kesesuaiannya dalam hasil analisis dan perancangan yang diharapkan, sehingga sistem dapat berfungsi dengan optimal. Pengujian ini penting sebagai tolok ukur untuk mencapai tujuan tersebut. Metode pengujian blackbox testing digunakan untuk mendeteksi kesalahan dan mengevaluasi kinerja sistem saat dijalankan. Metode ini memastikan bahwa input diterima dengan benar dan output yang dihasilkan sesuai dengan yang diharapkan.

3. HASIL DAN PEMBAHASAN

3.1. Spesifikasi Basis Data

Tabel 1 dan Tabel 2 adalah susunan spesifikasi basis data yang mana diterapkan dalam pembuatan aplikasi pengamanan *file*.

Tabel 1. *File*

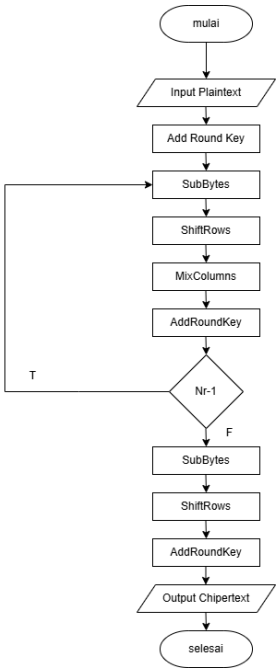
Nama	Type	Ukuran	Keterangan
id_file	*int*	11	Id_*file*
Username	*varchar*	15	*Username*
file_name_source	*varchar*	255	Nama asli *file*
file_name_finish	*varchar*	255	Nama hasil *file*
file_url	*varchar*	255	Url *file*
file_size	*float*	-	Ukuran *file*
Password	*varchar*	16	*Password*
tgl_upload	*date&time*	-	Tanggal upload
Status	*enum*	(‘1’,’2’)	Enkripsi dan dekripsi
Keterangan	*varchar*	255	Keterangan
durasi enkripsi	*varchar*	255	Waktu enkripsi

Tabel 2. *Users*

Nama	Type	Ukuran	Keterangan
Username	*varchar*	15	*Username*
Password	*varchar*	100	*Password*
Fullname	*varchar*	50	Nama *user*
job_title	*varchar*	50	Jabatan
last_activity	*timestamp*	-	Aktivitas terakhir

3.2. *Flowchart* Enkripsi AES-128

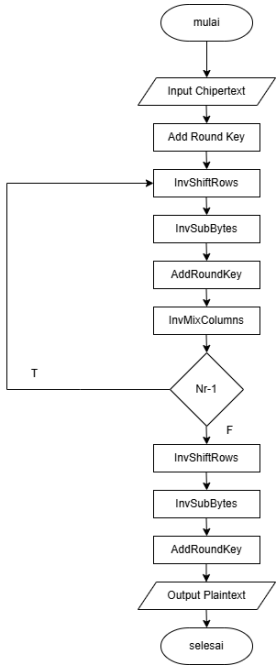
Menjelaskan langkah demi langkah untuk proses enkripsi *Plaintext*. Gambar 3 menunjukkan *flowchart* proses enkripsi AES-128.



Gambar 3. *Flowchart* Proses Enkripsi AES-128

3.3. *Flowchart* Dekripsi AES-128

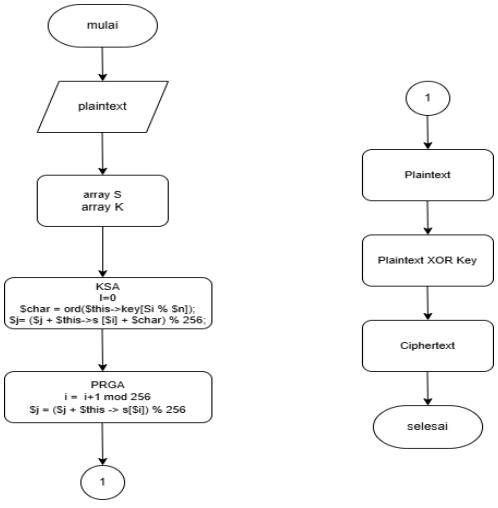
Menjelaskan langkah demi langkah untuk proses dekripsi guna mengembalikan *chipertex*t menjadi teks asli. Gambar 4 menunjukkan *flowchart* proses dekripsi AES-128.



Gambar 4. *Flowchart* Proses Dekripsi AES-128

3.4. *Flowchart* Enkripsi RC4

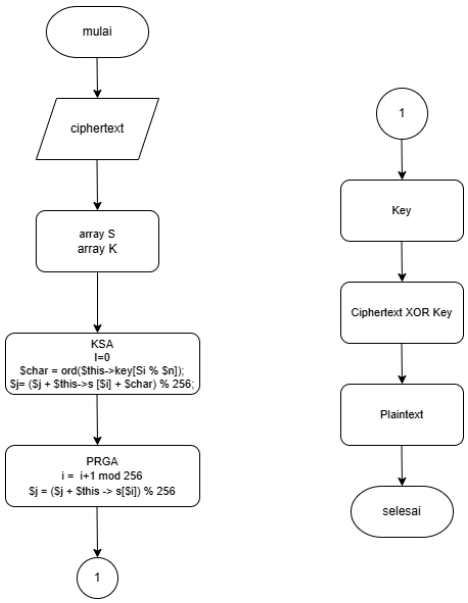
Dimulai dengan inisialisasi input berupa *array* S dan *array* K. Selanjutnya, dilakukan tahap *Key Scheduling Algorithm* (KSA) yang kemudian diikuti oleh tahap *Pseudo-Random Generation Algorithm* (PRGA), yang menghasilkan sebuah kunci. Tahap berikutnya adalah proses enkripsi, di mana *plaintext* di-XOR dengan kunci yang telah terbentuk. Hasil akhirnya adalah *ciphertext*. Gambar 5 menunjukkan *flowchart* enkripsi RC4



Gambar 5. *Flowchart* Enkripsi RC4

3.5. *Flowchart* Dekripsi RC4

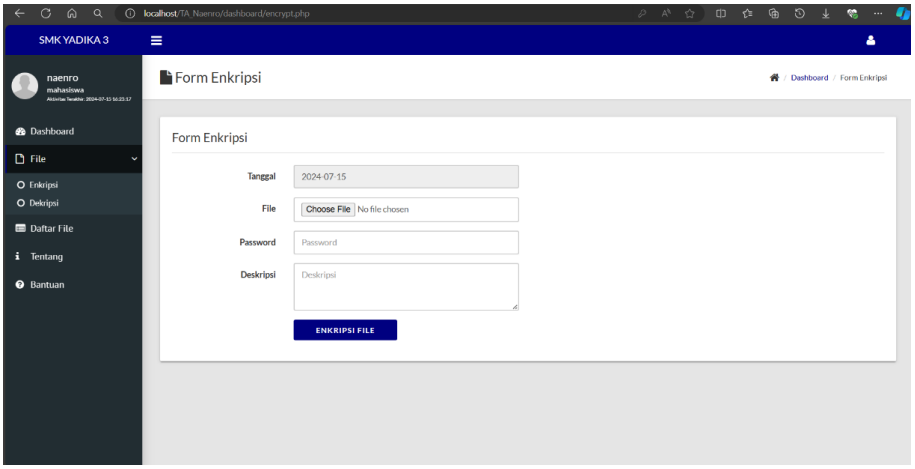
Proses dekripsi mirip dengan enkripsi RC4, langkah-langkah pembentukan kunci dilakukan terlebih dahulu. Setelah kunci terbentuk, proses dekripsi dilakukan dengan meng-XOR-kan *ciphertext* dengan kunci tersebut. Proses ini menghasilkan teks asli. Gambar 6 menunjukkan *flowchart* proses dekripsi RC4.



Gambar 6. *Flowchart* Dekripsi RC4

3.6. Tampilan Layar Halaman Enkripsi

Halaman Gambar 7, halaman yang digunakan untuk melakukan proses enkripsi *file* yang diinginkan. Pada laman ini, tersedia tombol untuk memilih berkas *file* yang ingin dienkripsi, serta *form* untuk memasukkan kata sandi dan deskripsi untuk *file* tersebut. Button "Enkripsi *File*" memiliki fungsi untuk memproses dokumen yang dienkripsi. Gambar 7. Menunjukkan Tampilan Layar Halaman Enkripsi.

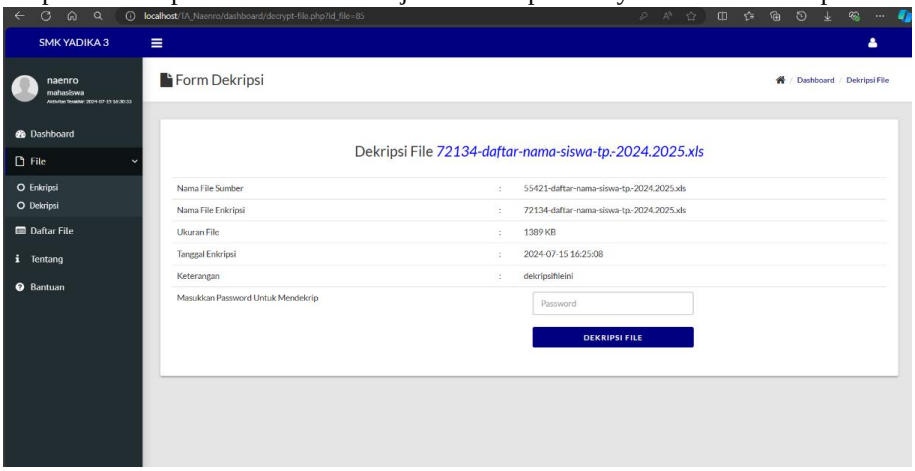


Gambar 7. Tampilan Layar Halaman Enkripsi

a. *File* yang berukuran kecil (53.1 KB) seperti pada *file* "43689-soal-bahasa-inggris.docx ", memiliki waktu enkripsi yang lebih cepat yaitu (0,643 detik).
b. *File* yang berukuran besar 3.76 MB, seperti pada *file* "34731-soal-essay-assesmen-sumatif-sekolah-2023-2024.docx", membutuhkan waktu enkripsi yang lebih lama yaitu (91.062 detik).
c. Proses enkripsi menggunakan algoritma AES-128 terlebih dahulu, lalu dilanjut dengan RC4, semakin lama durasi waktu enkripsinya tergantung pada ukuran *file*.
d. *File* dengan format Word, Excel dan PDF, berhasil terenkripsi menggunakan password yang ditentukan oleh *user* dan isi pada *file* menjadi acak dan tidak dapat dibaca oleh pihak yang tidak berkepentingan.
e. *File* yang sudah terenkripsi tidak mengalami perubahan pada nama *file*, ukuran file dan format *file*.

3.7. Tampilan Layar Halaman Dekripsi

Halaman Gamabr 8, untuk menjalankan proses dekripsi *file*, *user* perlu *input* kata sandi yang sama seperti yang digunakan saat proses enkripsi. Gambar 8 menunjukkan Tampilan Layar Halaman Dekripsi.



Gambar 8. Tampilan Layar Halaman Dekripsi

3.8. Pengujian

Pada tahap ini dilakukan pengujian terhadap aplikasi yang telah dibuat untuk mengetahui ukuran *file* hasil proses enkripsi dan dekripsi dari metode *Advanced Encryption Standard* (AES) 128 dan *Rivest Code 4* apakah berbeda atau sama, lalu untuk mengetahui juga berapa lama waktu proses enkripsi dan dekripsi *file*. Berikut Tabel 3 dan Tabel 4 adalah hasil dari proses enkripsi dan dekripsi *Advanced Encryption Standard* (AES) 128 dan *Rivest Code 4*.

Tabel 3. Hasil Pengujian Enkripsi

Nama File	Password	Ukuran File	Waktu Enkripsi	Output File
43689-soal-bahasa-inggris.docx	9876543211234567	55.1 KB	0.643 detik	78334-soal-bahasa-inggris.docx
97394-daftar-nama-siswa-tp.-2024.2025.xls	1234567891234567	1.35 MB	14.934 detik	33982-daftar-nama-siswa-tp.2024.2025.xls
52998-daftar-nilai-akhir-sekolah.pdf	disekolahyadika3	2.42 MB	29.881 detik	28769-daftar-nilai-akhir-sekolah.pdf
34731-soal-essay-assesmen-sumatif-sekolah-2023-2024.docx	disekolahyadika3	3.76 MB	91.062 detik	21541-soal-essay-assesmen-sumatif-sekolah-2023-2024.docx

Berdasarkan Tabel 3, Hasil analisanya dapat disimpulkan sebagai Tabel 4 berikut:

Tabel 4. Hasil Pengujian Dekripsi

Nama File	Password	Ukuran File	Waktu Dekripsi	Output File
43689-soal-bahasa-inggris.docx	9876543211234567	55.1 KB	0.536 detik	43689-soal-bahasa-inggris.docx
33982-daftar-nama-siswa-tp.2024.2025.xls	1234567891234567	1.35 MB	13.418 detik	97394-daftar-nama-siswa-tp.-2024.2025.xls
28769-daftar-nilai-akhir-sekolah.pdf	disekolahyadika3	2.42 MB	28.287 detik	52998-daftar-nilai-akhir-sekolah.pdf
34731-soal-essay-assesmen-sumatif-sekolah-2023-2024.docx	disekolahyadika3	3.76 MB	90.105 detik	34731-soal-essay-assesmen-sumatif-sekolah-2023-2024

Berdasarkan Tabel 4 pengujian dekripsi di atas, hasil analisanya dapat disimpulkan sebagai berikut:

a. *File* yang berkapasitas kecil (53.1 KB), seperti pada *file* "43689-soal-bahasa-inggris.docx", memiliki waktu dekripsi yang sangat cepat yaitu (0,636 detik).
b. *File* yang berkapasitas besar 3.76 MB, seperti pada *file* "34731-soal-essay-assesmen-sumatif-sekolah-2023-2024.docx", membutuhkan waktu dekripsi yang lebih lama yaitu (90.105 detik).
c. Masukan *password* yang digunakan pada saat proses enkripsi, untuk mendekripsi atau mengembalikan *file* ke dalam bentuk aslinya yang dapat dibaca.

d. Sama seperti saat proses enkripsi, nama *file*, ukuran *file*, dan format *file* tidak mengalami perubahan.
e. Menggunakan algoritma RC4 lalu dilanjut AES-128 saat proses dekripsi, lebih cepat 1 detik.

4. KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap masalah serta pengujian aplikasi, hasil implementasi aplikasi keamanan *file* menggunakan algoritma *Advanced Encryption Standard (AES-128)* dan *Rivest Code 4* (RC4) menunjukkan bahwa proses enkripsi dan dekripsi dokumen *file* berhasil melindungi *file* dokumen di SMK Yadika 3 dari kebocoran data. Kecepatan proses enkripsi dan dekripsi juga bergantung pada kapasitas *file* dokumen yang diproses. Saran untuk peneliti selanjutnya agar dapat dikembangkan lebih baik lagi yaitu mampu mengenkripsi format *file* suara, gambar, video, sms dan format lainnya, dapat ditambahkan metode lain seperti steganografi untuk menyisipkan sebuah *file* dokumen kedalam *file* dokumen lain, untuk mengamankan data dari pihak yang tidak bertanggung jawab, dan dapat meningkatkan kapasitas penyimpanan untuk proses enkripsi *file*.

DAFTAR PUSTAKA

[1] F. A. Nurbi and U. Budiyanto, "Penerapan Algoritme Rivest Code 4 Untuk Pengamanan Dokumen Di CV. Bintang Pratama Mandiri," Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), Vol. 1, No. 1, pp. 182-192, 2022.
[2] Herman, R. Wijaya, S. Miharja, and Wilson, "Implementasi Algoritma Aes-128 Dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen," *J. TIMES*, vol. 10, no. 2, pp. 80–87, 2021, [Online]. Available: https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/666
[3] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.
[4] J. Syahputra Sianipar, N. Budi Nuugroho, I. Mariami, S. Informasi, and S. Triguna Dharma, "Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode Advanced Encryption Standard (AES)," *J. Sist. Inf. Tgd*, vol. 3, no. 1, pp. 35–45, 2024, [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jsi
[5] Z. Basim and Painem, "Implementasi Kriptografi Algoritma Rc4 Dan 3Des Dan Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As-Su'Udiyyah," *Skanika*, vol. 3, no. 4, pp. 54–60, 2020.
[6] S. D. Nurcahya, "Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 4, pp. 694–697, 2022, doi: 10.32672/jnkti.v5i4.4690.
[7] P. Rusyandi and R. Pradana, "Aplikasi Kriptografi Berbasis Web System Menggunakan Algoritma Aes-128 Untuk Keamanan File Ujian Siswa Smk Cengkareng 1 Jakarta Cryptography Applications Based Of Web System An Using Aes-128 Algorithm For Exam File Security Students At Smk Cengkareng 1," Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), vol. 3, no. April, pp. 9–19, 2024.
[8] R. A. Umar and S. Hari, "Implementasi Algoritma Rc4 Untuk Keamanan File Berbasis Web Pada Sdit Ar Rahman," Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), vol. 1, no. 1, pp. 377–385, 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index
[9] W. Wahyudi, D. Hartama, I. O. Kirana, S. Sumarno, and I. Gunawan, "Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun," *J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 57–66, 2022, doi: 10.54082/jiki.19.
[10] A. T. Pandya and J. C. Chandra, "Aplikasi Keamanan File Menggunakan Algoritme Kriptografi Aes 128 Berbasis Web Pada Pilar Medical Center," Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), vol. 2, no. 2, pp. 36–45, 2023.