Insearch
Information System Research Journal

E-ISSN: 2775-4669
Volume 5, Nomor 1, Februari 2025

Implementasi Kriptografi Keamanan Dokumen Desa Menggunakan Metode *Rivest Code* 4 (RC4) di Balai Desa Banyuanyar

Fadila Afga Arian[1], Yudo Bismo Utomo[2], Halimahtus Mukmina[3]
Teknik Komputer, Universitas Islam Kadiri, Indonesia
Jl. Sersan Suharmaji No.38, Manisrenggo, Kec. Kota, Kota Kediri, Jawa Timur 64128
E-mail: fadilaafga69@gmail.com[1], yudobismo@uniska-kediri.ac.id[2], halimahtusm@uniska-kediri.ac.id[3]

Received: 13 Nov 2024 | Revised: 23 Jan 2025
Accepted: 28 Jan 2025 | Published: 28 Feb 2025

Abstrak

Keamanan dokumen di Balai Desa Banyuanyar sangat penting untuk melindungi data sensitif seperti surat kehilangan, keterangan domisili, dan dokumen keuangan. Observasi menunjukkan bahwa dokumen saat ini hanya disimpan dalam format soft file tanpa keamanan yang cukup, sehingga berisiko diakses oleh pihak tidak berwenang. Penelitian ini mengimplementasikan algoritma enkripsi simetris RC4 melalui aplikasi web "SEKEDAB" (Sistem Keamanan Dokumen Banyuanyar) untuk mengenkripsi dan mendekripsi dokumen dalam format .docx, .pdf, .xlsx, dan .pptx. Pengujian menunjukkan bahwa aplikasi ini dapat mengenkripsi dan mendekripsi dokumen dengan cepat dan efisien, dengan rata-rata waktu enkripsi 0,46 detik dan dekripsi 0,45 detik untuk dokumen 1 MB.

Kata kunci: Kriptografi, Keamanan Dokumen, RC4

Abstract

Document security at Banyuanyar Village Office is essential to protect sensitive data such as loss certificates, domicile certificates, and financial documents. Observations show that these documents are currently stored as soft files without adequate security, making them vulnerable to unauthorized access. This study implements the RC4 symmetric encryption algorithm through a web application called "SEKEDAB" (Banyuanyar Document Security System) to encrypt and decrypt documents in .docx, .pdf, .xlsx, and .pptx formats. Testing showed that this application can encrypt and decrypt documents quickly and efficiently, with an average encryption time of 0.46 seconds and decryption time of 0.45 seconds for a 1 MB document.

Keywords: Cryptography, Document Security, RC4

I. PENDAHULUAN

Sebagai salah satu lembaga pemerintahan ditingkat desa, Balai Desa Banyuanyar memiliki kewajiban menjaga keamanaan dokumen dan surat penting yang ada di desa, dokumen dan surat penting desa mencakup berbagai informasi penting seperti surat kehilangan, surat keterangan domisili dan juga dokumen keuangan desa. Keamanan dan kerahasiaan informasi menjadi aspek yang sangat dijaga agar data data penting tidak mudah disalahgunakan oleh pihak yang tidak memiliki izin. Menurut observasi di lokasi, peneliti menemukan bahwa file dokumen di Balai Desa Banyuanyar tidak memiliki keamanan dan hanya disimpan berupa soft file sehingga bisa dengan bebas di akses pihak yang tidak memiliki izin. Beberapa ancaman yang diberikan adalah masalah keamanan, kerahasiaan, dan keaslian data. untuk memastikan bahwa data atau pesan tidak dapat dibaca oleh orang yang tidak berwenang, dan juga mencegah mereka mengubah, menghapus, atau memasukkan elemen yang tidak pantas yang

mengganggu keaslian data [1]. Salah satu cara ialah menambah kriptografi. Kriptografi adalah ilmu yang digunakan untuk menjaga keamanan pesan. Lebih dalamnya, kriptografi adalah tentang teknik matematika yang berkaitan dengan elemen keamanan data seperti kerahasiaan, integritas, dan otentikasi. *Plaintext*, yang merupakan pesan sumber pertama yang dapat dibaca oleh semua orang, disebut sebagai *cipherteks* dalam mengamankan data, sedangkan *cipherteks* adalah bentuk pesan yang sudah disandikan atau terenkripsi yang telah diubah dari *plainteks* agar lebih aman dan tidak dapat dibaca oleh publik. Dalam kriptografi, dua proses utama adalah enkripsi dan deskripsi. Enkripsi mengubah *plainteks* menjadi *cipherteks*, dan deskripsi mengubah *cipherteks* menjadi *plainteks*.[2]. Menurut penelitian yang dilakukan oleh Wardhana F, Kurniawan A, Seto B yang membandingkan algoritma RC4 dan AES hasil menunjukkan bahwa RC4 memiliki kecepatan enkripsi lebih baik, sementara AES memerlukan waktu lebih lama. Ukuran file enkripsi dengan RC4 tetap sama, sedangkan AES menghasilkan ukuran yang berbeda. Kesimpulannya, pemilihan antara RC4 dan AES harus mempertimbangkan keseimbangan antara keamanan dan efisiensi, dengan pertimbangan khusus terkait waktu enkripsi dan ukuran file[3].

II. TINJAUAN PUSTAKA

A. Studi Literatur

a. Setelah mengumpulkan informasi dari penelitian sebelumnya yang berkaitan dengan peneliti yang menggunakan rivest code 4, beberapa penelitian serupa ditemukan untuk dijadikan refrensi tambahan. Penelitian ini dilakukan oleh Ketut Agus Seputra dan Gede Arna Jude Saskara yang berjudul "Kriptografi Simetris RC4 Pada Transaksi Booking Engine System" menyatakan bahwa perkembangan industri pariwisata di Bali membawa dampak pada makin meningkatnya persaingan bisnis pariwisata di Bali. Persaingan dapat terlihat dari munculnya agent-agent wisata baru di Bali. Untuk dapat bertahan dalam persaingan industri pariwisata, pelaku pariwisata tersebut harus mampu memanfaatkan peluang dalam meraih keuntungan dengan cara mengoptimalkan efektivitas pemasaran dan keuntungan. Salahsatu cara yang dapat ditempuh adalah dengan penjualan/transaksi paket wisata secara online melalui internet booking engine system (BES). Terdapat isu utama dalam aktivitas transaksi secara online, yaitu masalah keamanan informasi. Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Penerapan keamanan informasi khususnya dalam transaksi paket wisata online dapat berupa penggunaan metode kriptografi menggunakan algoritma RC4. Keefektifan dan kemudahan pemrosesan, membuat algoritma RC4 mudah dan ringan untuk diimplementasikan. Algoritma RC4 diimplementasikan guna melakukan enkripsi data pelanggan yang disimpan dalam basis data. Informasi yang sudah disimpan tersebut akan ditampilkan kembali ke plaintext melalui proses dekripsi menjadi informasi yang sebenarnya[4].

b. Adapun jurnal lain yang berjudul "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Voting Pemilihan Ketua Umum
Berbasis WEB" yang ditulis oleh Fadlilah Septyana Yanuba, Muhlis Tahir, M. Khamdi Fadli, Fathin Nisa Nafasa, Siti Aminatus Zahrah, Afifatur Rohmah menyatakan bahwa kemajuan teknologi yang sangat pesat terus mengalami perubahan dan pembaruhan yang lebih baik. Salah satu contohnya yakni pada sistem pemilihan umum, baik dari sebuah organisasi kecil maupun besar, yang dimana sebelumnya dilakukan dengan cara pemilihan langsung yakni dengan melakukan pemungutan suara menggunakan kertas suara. Pemilihan ini mengalami perubahan yang dilakukan melalui media online. Maka dari itu diperlukan pengamanan yang sangat baik agar data hasil pemilihan bisa tersimpan dengan baik tanpa adanya kecurangan yang dapat merusak hasil pemungutan suara. Pada saat pemilih mau menggunakan hak suaranya kerap kali ditemukan kasus jika pemilih tersebut bahwasannya sudah memilih padahal yang sebenarnya belum melaksanakan hak suaranya. Dengan adanya permasalahan tersebut, maka diperlukan suatu algoritma enkripsi untuk mengamankan akun dari pemilih yang mana nantinya algoritma ini akan dienkripsi pada hanya satu field saja yaitu password. sehingga pihak yang tidak bertanggung jawab atas keamanan database

tidak dapat membaca ataupun mengetahui karena privasi data tersebut. Algoritma yang digunakan yakni algoritma RC4[5].

c. Penelitian yang ditulis oleh Widiarti Rista Maya, Azanuddin,dan Elfitriani yang berjudul "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES" menyatakan bahwa Perkembangan teknologi pada era digital saat ini, komputer digunakan untuk membantu dan mempercepat kinerja manusia, salah satunya dengan melakukan pengamanan data. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi dan steganografi. Keamanan data nilai siswa sangat penting agar pihak yang tidak berkepentingan tidak akan membaca dan memanipulasi data nilai siswa tersebut. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada data nilai siswa dengan melakukan perhitungan algoritma Data Encryption Standard (DES). Algoritma Data Encryption Standard (DES) adalah algoritma cipher blok yang digunakan untuk keamanan informasi dengan menggunakan metode simetrik dalam mengenkripsi dan dekripsi data ataupun informasi. Hasil dari penelitian ini diharapkan dapat memberikan manfaat dan solusi kepada SD Negeri 064979 Medan untuk mengamankan data nilai siswa yang di input oleh guru sehingga meminimalkan kemungkinan untuk dibaca maupun dimanipulasi oleh pihak yang tidak berkepentingan[6].

d. Penelitian yang berjudul "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis WEB Pada PT. Trans Intra Asia" yang ditulis Andre Setiawan dan Titin Fatimah menyatakan bahwa saat ini data menjadi sangat penting bagi perusahaan. Banyak perusahaan menggunakan teknologi database untuk menyimpan banyak data perusahaannya. Keamaanan data yang di simpan ke dalam database sudah menjadi hal yang dibutuhkan. Namun keamanan database tidak dapat menjamin keamanan data karena kemanan data yang kurang baik sehingga dapat digunakan oleh pihak-pihak yang berhubungan dengan database seperti data penggajian. Perkembangan penggunaan database berbarengan dengan keharusan pemahaman akan keamanan database. Masih banyak lembaga atau instansi yang mengabaikan keamanan database, sehingga data yang ada bisa diakses oleh orang yang tidak bertanggung jawab. Banyak cara yang dilakukan untuk bisa mengamankan data tersebut. Algoritma RC4 termasuk kedalam kriptografi kunci simetris, yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kelebihan kunci simetris adalah untuk proses enkripsi dan dekripsi dibutuhkan waktu yang cukup singkat, untuk ukuran kunci simetris relative lebih pendek dan dapat dipergunakan untuk membangunkan bilangan acak, kunci simetris disusun untuk menghasilkan cipher yang lebih kuat[7].

e. Penelitian yang berjudul "Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigenere Chiper" yang ditulis oleh Risna, Yusni Amaliah, dan Selly Yunita menyatakan bahwa Keamanan data merupakan sebuah bentuk untuk memproteksi hal penting dalam hal ini data dari manipulasi atau penyalahgunaan oleh orang-orang yang tidak berwenang. CV Harapan Kaltim Abadi merupakan distributor yang bergerak dibidang peralatan dan kosmetika yang belum memiliki metode pengamanan data pembayaran pelanggan, sehingga sangat rentan terhadap manipulasi dan memungkinkan terjadinya kebocoran data dan manipulasi data. Solusi yang dapat digunakan untuk mencegah hal tersebut yaitu ilmu kriptografi, yaitu ilmu penyandian data. Vigenere Cipher ialah salah satu metode dalam kriptografi. Metode ini mengubah kalimat asli melalui urutan Caesar cipher mengacu pada huruf dalam kata kunci. Proses enkripsi pada penelitian ini menggunakan Vigenere Cipher yang menerapkan metode kriptografi kunci simetris. Proses enkripsi dan deskripsi dalam kriptografi dengan kata kunci simetris hanya membutuhkan satu kunci. Kunci yang digunakan dalam proses enkripsi dan deskripsi adalah kunci yang sama. Plaintext berubah menjadi ciphertext dengan kata-kata yang tidak dapat dipahami. Pada proses deskripsi, ciphertext berubah kembali menjadi plaintext, yaitu teks yang dapat dibaca kembali. Berdasarkan penerapan dan proses uji coba yang dilakukan dalam penelitian ini, metode Vigenere Cipher telah berhasil mengamankan

data pembayaran piutang pelanggan berupa file Microsoft Excel yang berisi satu sampai dua lembar dokumen. Tahapan penyandian atau enkripsi dan pengembalian atau deskripsi dilakukan dengan menggunakan karakter yang berisi non-huruf kapital, huruf kapital dan simbol sesuai dengan jumlah karakter pada keyboard[8].

B. Kriptografi

Kriptografi berasal dari kata Yunani "*cryptos*", yang berarti "rahasia", dan "*graphein*", yang berarti "tulisan". Kriptografi, oleh karena itu, adalah seni dan ilmu untuk mengamanan pesan. Proses enkripsi dan dekripsi adalah dua konsep utama dalam kriptografi. Enkripsi adalah proses pengiriman data atau informasi yang kemudian diubah menjadi bentuk yang sulit diketahui sebagai informasi menggunakan algoritma tertentu. Dikenal sebagai "*plaintext*", dekripsi adalah proses mengubah informasi yang tersamar menjadi informasi yang asli dan tidak diubah. Kemudian, setelah disamarkan oleh kriptografi, *plaintext* disebut sebagai *ciphertext*. Mengubah *plaintext* menjadi *ciphertext* disebut enkripsi, dan mengembalikannya ke plaintext disebut dekripsi.[9].

C. Algoritma Rivest Code 4 (RC4)

RC4 adalah jenis aliran kode yang memungkinkan operasi enkripsi dilakukan per satu karakter untuk satu operasi. RSA Data Security Inc. (RSADSI) membuat algoritma kriptografi Rivest Code 4 (RC4), yang diciptakan oleh Ronald Rivest pada tahun 1987 dan menjadi simbol keamanan RSA (Rivest Shamir Adleman)[10].

0	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
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

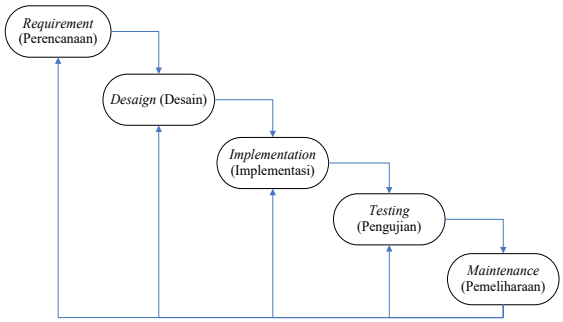
Gambar 1 Nilai S-Box

C4 menggunakan dua S-Box, atau kotak substitusi, array 256 byte. Satu S-Box memiliki permutasi dari 0 hingga 255, dan yang lain memiliki permutasi fungsi dari kunci dengan panjang yang berubah-ubah. Algoritma RC4 memulai S-box pertama, S[0], S[1],..., S[255], yang terdiri dari 0 hingga 255, secara berurutan dengan nilai S[0] = 0, S[1] = 1,..., S[255] = 255. Kemudian memulai array lain (S-Box lain), misalnya array K dengan panjang 256, dan mengisi array K dengan kunci yang diulangi sampai seluruh array S[0], K[1],..., K[255] terisi sepenuhnya[11].

III. METODE PENELITIAN

Metode yang digunakan untuk membuat aplikasi keamanan file dokumen desa menggunakan metode rivest code 4 (RC4) di Balai Desa Banyuanyar ini adalah metode waterfall. Metode waterfall, yang menyajikan tahap demi tahap, sangat sesuai dengan keadaan di lapangan. Oleh karena itu, metode ini layak diterapkan untuk melakukan penelitian ini[12]. Keuntungan dari metode waterfall ini adalah fokus diselesaikan terlebih dahulu di setiap tahapannya, sehingga pengerjaannya dilakukan secara maksimal dan tidak adanya pengerjaan secara parallel[13].

Berikut ini tahapan metode waterfall:



Gambar 2 Metode *Waterfall*

A. Perencanaan

Dalam proses pengerjaan ini memiliki tujuan untuk memperoleh hasil yang akurat dan sesuai kebutuhan, untuk mendapatkan hasil yang diinginkan penelitian ini menggunakan metode kualitatif dan deskriptif. Penelitian kualitattif adalah penelitian yang menggunakan pendekatan *naturalistic* untuk mencari dan menemukan pengertian atau pemahaman tentang fenomena dalam suatu latar yang berkonteks khusus[14]. Metode pengumpulan data dalam penelitian kualitatif meliputi observasi, wawancara, dan studi literatur.

Pertama observasi, observasi dilakukan dengan cara pengamatan langsung terhadap data di lapangan, mulai dari pengenalan data hingga pengolahan data, sehingga data tersebut dapat membantu penelitian yang mendeskripsikan kondisi di lapangan.

Kedua wawancara, wawancara dilakukan langsung dengan pihak yang berkepentingan, wawancara ini dilakukan kepada staf di balai desa Banyuanyar untuk memperoleh informasi, selain itu tujuan dari wawancara adalah untuk mendapatkan pendapat dan solusi terhadap masalah yang terjadi.

Ketiga studi literatur, studi literatur adalah metode yang digunakan untuk mencari dan mengumpulkan informasi yang relevan dengan penelitian yang dilakukan, selama proses ini peneliti mencari refrensi dan teori yang berkaitan dengan topik yang sedang dipelajari. Refrensi juga bertujuan untuk mengembangkan pemahaman tentang topik tersebut dan memastikan bahwa skripsi disusun dengan baik dan didukung oleh literatur yang kuat

B. Analisa Kebutuhan Sistem

Kebutuhan sistem dihasilkan berdasarkan hasil pengamatan terhadap permasalahan yang terjadi di balai desa Banyuanyar, sehingga pengimplementasian aplikasi keamanan file dokumen ini dapat mengatasi permasalahan yang ada di balai desa Banyuanyar dan dapat diimplementasikan dengan baik agar file dokumen yang ada pada balai desa Banyuanyar dapat terjaga dengan baik dan aman. Berikut adalah analisis terhadap aplikasi yang akan diimplementasikan :

Fitur pada sistem :

1. Sistem dapat menampilkan form halaman login dan tampilan utama.
2. Sistem dapat mengenkripsi file dokumen.
3. Sistem dapat mengdeskripsi file yang sudah di enkripsi.
4. Sistem dapat mengunduh dokumen yang telah di enkripsi dan di dekripsi.
5. Sistem dapat menghapus list file dokumen yang telah di enkripsi dan di dekripsi.

Fitur pada Admin :

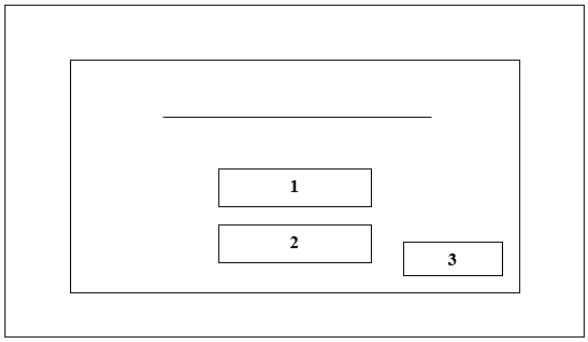
1. Admin dapat menyimpan dokumen yang telah di enkripsi dan di dekripsi.
2. Admin dapat mengunduh file dokumen yang telah di enkripsi dan di dekripsi.
3. Admin dapat menghapus list dokumen yang telah di enkripsi

C. Rancangan Desain Aplikasi (*Wireframe*)

Desain aplikasi biasanya berisi penjelasan secara singkat tentang bagaimana aplikasi yang akan dikembangkan akan terlihat dan bekerja. Ringkasan ini berisi informasi tentang tampilan, fitur, dan fungsionalitas, serta alur kerja aplikasi. Berikut adalah desain aplikasi[15] :

1) Halaman *Login*

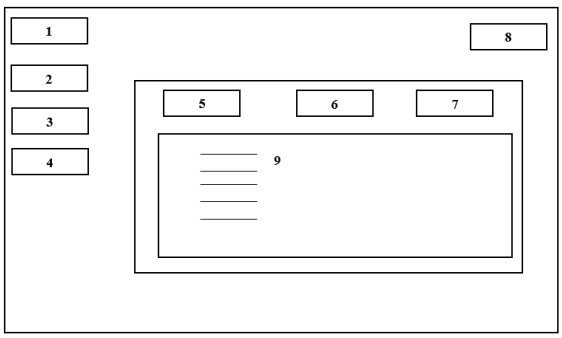
Admin harus memasukan *username* dan *password* yang benar untuk masuk ke aplikasi. Terlihat pada gambar 3.



Gambar 3 Halaman *Login*

2) Halaman Utama atau *Dashboard*

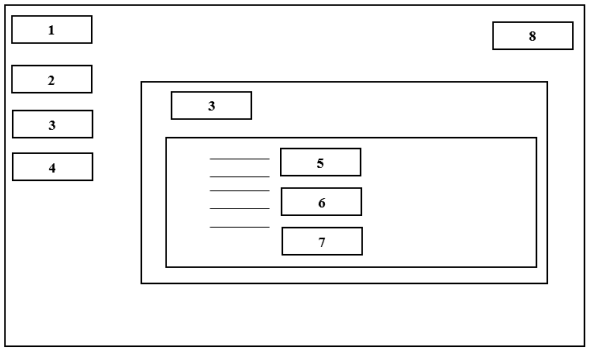
Setelah berhasil melakukan *login* maka akan menampilkan halaman *dashboard* atau halaman utama yang berisi *list* dokumen, tombol *download* dokumen, tombol hapus dokumen, *menu* enkripsi, dan *menu* dekripsi. Terlihat pada gambar 4.



Gambar 4 Halaman Utama

3) *Menu* Enkripsi

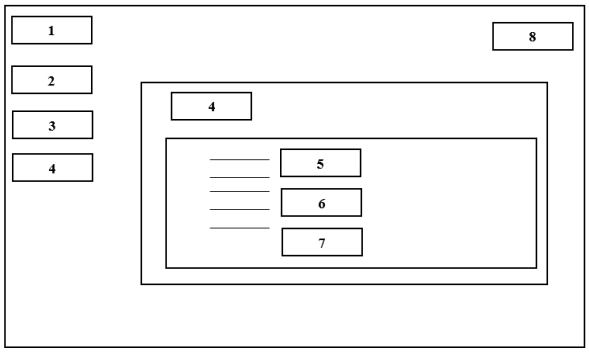
Didalam *menu* enkripsi kita dapat melakukan proses enkripsi terhadap dokumen yang diperlukan. Terlihat pada gambar 5.



Gambar 5 *Menu* Enkripsi

4) *Menu* Dekripsi

Didalam *menu* dekripsi kita dapat melakukan *proses* dekripsi terhadap dokumen yang sudah dienkripsi dengan memasukan *key* yang sama dengan *key* enkripsi. Terlihat pada gambar 6.



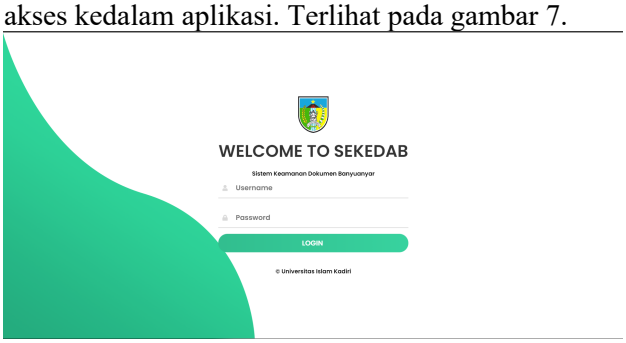
Gambar 6 *Menu* Dekripsi

IV. HASIL DAN PEMBAHASAN

A. Hasil Implementasi

1) Tampilan *Login*

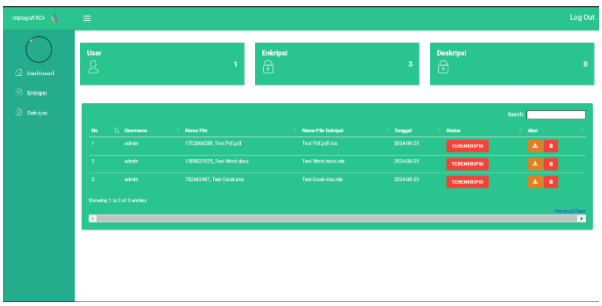
Tersedia form untuk melakukan pengisian username dan password untuk masuk ke dalam aplikasi, agar dapat menggunakan fitur yang tersedia dalam aplikasi. Login diperlukan untuk memverifikasi apakah pengguna mempunyai hak akses kedalam aplikasi. Terlihat pada gambar 7.



Gambar 7 Halaman *Login*

2) Tampilan *Dashboard.*

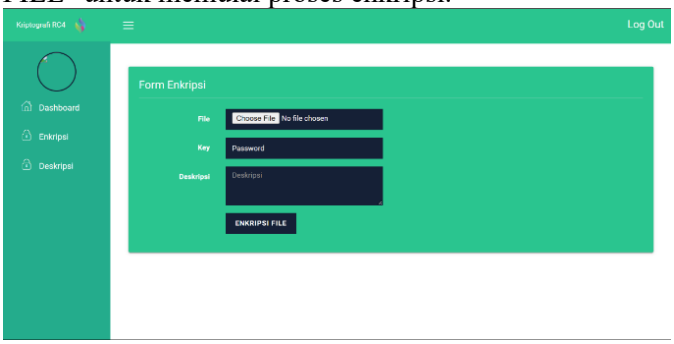
Pada tampilan halaman utama seperti pada gambar 8, terdapat sidebar, yang memiliki beberapa menu navigasi seperti tombol "Dashboard" untuk kembali ke halaman utama, menu "Enkripsi" untuk mengakses fitur enkripsi file, serta menu "Dekripsi" untuk mengakses fitur dekripsi file. Selain itu, di halaman utama, ditampilkan informasi mengenai jumlah pengguna, jumlah enkripsi yang telah dilakukan, serta jumlah dekripsi yang ada. Bagian tabel di bawahnya menyediakan tempat untuk menampilkan data file yang sudah dienkripsi atau sudah didekripsi dan juga dapat melakukan download file dan menghapus file.



Gambar 8 Tampilan *Dasboard*

3) Tampilan *Menu* Enkripsi

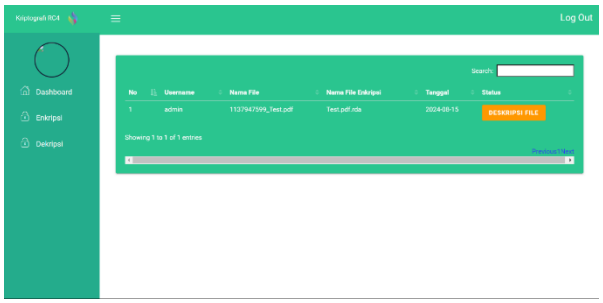
Pada gambar 9, pengguna dapat melakukan enkripsi file dengan memasukkan beberapa informasi. Di bagian ini, terdapat tiga kolom input yang pertama adalah kolom untuk memilih file yang akan dienkripsi, yang kedua adalah kolom untuk memasukkan kunci (*password*) yang akan digunakan dalam proses enkripsi, dan yang ketiga adalah kolom opsional tidak wajib diisi yaitu kolom deskripsi untuk menambahkan keterangan terkait file yang akan dienkripsi. Setelah memilih file dan memasukan *password* yang akan digunakan untuk menjalan proses enkripsi, pengguna dapat menekan tombol "ENKRIPSI FILE" untuk memulai proses enkripsi.



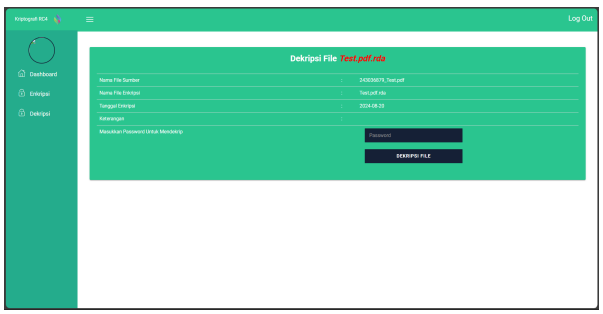
Gambar 9 Menu Enkripsi

4) Tampilan *Menu* Dekripsi

Pada gambar 10 menampilkan hasil dari proses enkripsi file. Pengguna dapat melihat daftar *file* yang telah dienkripsi, lengkap dengan detail seperti username, nama *file* asli, nama *file* hasil enkripsi, tanggal enkripsi, serta status. Terdapat juga tombol "DEKRIPSI FILE" yang memungkinkan pengguna untuk mendekripsi dokumen yang telah dienkripsi sebelumnya. Pada gambar 11 adalah tampilan untuk memasukan *password* untuk melakukan *proses* dekripsi.



Gambar 10 *Menu* Dekripsi



Gambar 11 *Menu* Dekripsi

2. Pengujian Rata-Rata Kecepatan

Setelah tahap implementasi sistem dilaksanakan serta mendapatkan hasil berupa aplikasi[15] dilakukan pengujian. Pengujian kecepatan dilakukan dengan dua metode yang pertama menggunakan ukuran file yang berbeda-beda dan yang kedua menggunakan ukuran file yang serupa. Untuk mengetahui waktu yang diperlukan untuk melakukan proses enkripsi dan dekripsi. Pengujian dilakukan menggunakan dokumen diluar milik balai desa karena terbatasnya jumlah file yang disediakan oleh pihak balai desa, dengan menggunakan dokumen tidak resmi diharapkan dapat melakukan pengujian yang lebih bervariasi.

1. Pengujian pertama menggunakan ukuran file yang berbeda-beda yang memiliki tujuan untuk mengetahui rata-rata waktu yang diperlukan untuk sekali proses enkripsi dan dekripsi.

Rumus untuk mengetahui rata-rata : Rata-rata= $\frac{Jumlah\ total\ semua\ waktu}{Jumlah\ data}$

Berikut hasil pengujian yang telah dilakukan :

Setelah mengumpulkan dokumen berformat word yang memiliki ukuran berbeda-beda dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 1.

Tabel 1 Rata-Rata Kecepatan Dokumen Word

Word	Ukuran	Waktu Enkripsi	Waktu Dekripsi
1.	123Kb	0.05 Detik	0.05 Detik
2.	201Kb	0.07 Detik	0.08 Detik
3.	178Kb	0.06 Detik	0.07 Detik
4.	291Kb	0.1 Detik	0.1 Detik
5.	227Kb	0.08 Detik	0.08 Detik
Rata-Rata :		0.072 Detik	0.076 Detik

Setelah mengumpulkan dokumen berformat pdf yang memiliki ukuran berbeda-beda dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 2.

Tabel 2 Rata-Rata Kecepatan Dokumen Pdf

Pdf	Ukuran	Waktu Enkripsi	Waktu Dekripsi
1.	298Kb	0.12 Detik	0.12 Detik
2.	1.068Kb	0.41 Detik	0.38 Detik
3.	340Kb	0.12 Detik	0.14 Detik
4.	679Kb	0.28 Detik	0.27 Detik
5.	718Kb	0.29 Detik	0.26 Detik
Rata-Rata :		0.24 Detik	0.23 Detik

Setelah mengumpulkan dokumen berformat excel yang memiliki ukuran berbeda-beda dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 3.

Tabel 3 Rata-Rata Kecepatan Dokumen Excel

Excel	Ukuran	Waktu Enkripsi	Waktu Dekripsi
1.	76Kb	0.03 Detik	0.03 Detik
2.	99Kb	0.03 Detik	0.04 Detik
3.	69Kb	0.03 Detik	0.03 Detik
4.	1.191Kb	0.45 Detik	0.45 Detik
5.	53Kb	0.02 Detik	0.02 Detik
Rata-Rata :		0.11 Detik	0.11 Detik

Setelah mengumpulkan dokumen berformat ppt yang memiliki ukuran berbeda-beda dilakukan

proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 4.

Tabel 4 Rata-Rata Kecepatan Dokumen Ppt

Ppt	Ukuran	Waktu Enkripsi	Waktu Dekripsi
1.	10.602Kb	4.16 Detik	4.25 Detik
2.	7.046Kb	2.83 Detik	2.81 Detik
3.	135Kb	0.05 Detik	0.05 Detik
4.	85Kb	0.03 Detik	0.04 Detik
5.	5.868Kb	2.34 Detik	2.33 Detik
Rata-Rata :		1.88 Detik	1.90 Detik

2. Pengujian kedua menggunakan file dengan ukuran yang serupa yaitu 1 Mb atau 1000 Kb yang memiliki tujuan untuk mengetahui rata-rata kecepatan yang dibutuhkan untuk melakukan enkripsi dan dekripsi.

Setelah mengumpulkan dokumen berformat word yang memiliki ukuran serupa yaitu 1Mb dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 5.

Tabel 5 Pengujian Dokumen Word

Word	Enkripsi	Dekripsi
1.	0.43 Detik	0.40 Detik
2.	0.44 Detik	0.38 Detik
3.	0.43 Detik	0.43 Detik

Setelah mengumpulkan dokumen berformat pdf yang memiliki ukuran serupa yaitu 1Mb dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 6.

Tabel 6 Pengujian Dokumen Pdf

Pdf	Enkripsi	Dekripsi
1.	0.43 Detik	0.42 Detik
2.	0.44 Detik	0.39 Detik
3.	0.43 Detik	0.41 Detik

Setelah mengumpulkan dokumen berformat excel yang memiliki ukuran serupa yaitu 1Mb dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 7.

Tabel 7 Pengujian Dokumen Excel

Excel	Enkripsi	Dekripsi
1.	0.47 Detik	0.41 Detik
2.	0.44 Detik	0.39 Detik
3.	0.46 Detik	0.39 Detik

Setelah mengumpulkan dokumen berformat ppt yang memiliki ukuran serupa yaitu 1Mb dilakukan proses enkripsi dan dekripsi yang menghasilkan waktu seperti pada tabel 8.

Tabel 8 Pengujian Dokumen Ppt

Ppt	Enkripsi	Dekripsi
1.	0.46 Detik	0.45 Detik
2.	0.45 Detik	0.43 Detik
3.	0.45 Detik	0.45 Detik

Jadi diketahui rata-rata waktu yang diperlukan untuk enkripsi dokumen dengan ukuran 1 Mb adalah 0.46 detik dan untuk dekripsi adalah 0.45 detik

V. KESIMPULAN

Berdasarkan hasil desain, implementasi, dan evaluasi yang telah dilakukan sesuai dengan rumusan masalah, maka kesimpulan yang dapat diambil adalah sebagai berikut.

1. Aplikasi Keamanan Dokumen Menggunakan Rivest Code 4 telah berhasil dirancang dan dikembangkan dengan menggunakan bahasa pemrograman PHP dan menggunakan aplikasi visual studio code untuk melakukan pemrograman dengan mengacu pada analisa kebutuhan serta desain awal yang telah dirancang. Pengujian fungsionalitas sudah dilakukan untuk mengetahui bahwa sistem bekerja dengan semestinya.
2. Implementasi kriptografi rivest code 4 (RC4) dalam aplikasi Keamanaan Dokumen telah berhasil dilakukan dan penulis juga sudah melakukan pengujian kecepatan rata-rata dalam proses enkripsi dan dekripsi dokumen, ada 4 dokumen yang memiliki format file berbeda yaitu .docx, .pdf, .xlsx, .pptx. Hasil menunjukan bahwa dengan ukuran dokumen 1 Mb membutuhkan rata-rata waktu enkripsi 0.46 detik dan untuk dekripsi membutuhkan waktu 0.45 detik.

REFERENSI

[1] B. Purba, F. Apustriani Gulo, N. Indah Utami, and Y. Annisa Sihotang, “Seminar Nasional Teknologi Komputer & Sains (SAINTEKS) Pengamanan File Teks Menggunakan Algoritma RC4,” *Semin. Nas. Teknol. Komput. Sains*, pp. 420–425, 2020.

[2] F. C. Manossoh, U. Budiyanto, and M. Hardjianto, “Pengamanan Dokumen Penjualan Perusahaan Menggunakan Algoritma Rc4 Pada Okiru Indonesia Securing Company Sales Documents Using the Rc4 Algorithm At Okiru Indonesia,” vol. 2, no. 1l, pp. 158–165, 2023.

[3] F. K. Wardhana, A. Kurniawan, B. R. Seto, and I. A. Saputro, “Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 Dan AES,” *Pros. Semin. Nas. AMIKOM SURAKARTA 2023*, no.

November, pp. 124–134, 2023.

[4] K. A. Seputra and G. A. J. Saskara, “Kriptografi Simetris RC4 Pada Transaksi Online Booking Engine System,” *J. Pendidik. Teknol. dan Kejuru.*, vol. 17, no. 2, pp. 286–295, 2020, [Online]. Available: https://ejournal.undiksha.ac.id/index.php/JPTK/article/view/27096

[5] F. S. Y. Arifah, M. Tahir, M. K. Fadli, F. N. Nafasa, S. A. Zahrah, and A. Rohmah, “Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Voting Pemilihan Ketua Umum Berbasis WEB,” *J. Inf. Syst.*, vol. 3, no. 1, pp. 1–9, 2023, doi: 10.61488/jis.v3i1.208.

[6] W. R. Maya, A. Azanuddin, and E. Elfitriani, “Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES,” *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 1, p. 1, 2022, doi: 10.53513/jis.v21i1.4764.

[7] A. Setiawan *et al.*, “KEAMANAN DATABASE APLIKASI PENGGAJIAN KARYAWAN,” vol. 4, no. 1, pp. 66–71, 2021.

[8] R. Risna, Y. Amaliah, and S. Yunita, “Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigenere Cipher,” *Sebatik*, vol. 26, no. 2, pp. 525–534, 2022, doi: 10.46984/sebatik.v26i2.2061.

[9] K. Fahmi, “Pengamanan Data Arsip Pada Balai Desa Sidodadi Menggunakan Kriptografi Modern RC4,” vol. 2, no. 2, pp. 58–66, 2021.

[10] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, and I. Gunawan, “Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4,” *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 114, 2020, doi: 10.30865/json.v1i2.1745.

[11] E. Listiyan and E. R. Subhiyakto, “Rancang Bangun Sistem Inventory Gudang Menggunakan Metode Waterfall Studi Kasus Di Cv. Aqualux Duspha Abadi Kudus Jawa Tengah,” *KONSTELASI Konvergensi Teknol. dan Sist. Inf.*, vol. 1, no. 1, pp. 74–82, 2021, doi: 10.24002/konstelasi.v1i1.4272.

[12] Y. B. Utomo, D. E. Yuliana, and H. Kurniadi, “Sistem Pendukung Keputusan Dalam Menentukan Ketua Himaprodi Menggunakan Metode Weighted Product,” *J. Tek. Inf. dan Komput.*, vol. 5, no. 2, p. 501, 2022, doi: 10.37600/tekinkom.v5i2.703.

[13] S. Hasibuan, I. Rodliyah, S. Z. Thalhah, P. W. Ratnaningsih, and A. A. M. S. E, *Media penelitian kualitatif*, vol. 5, no. January. 2022. [Online]. Available: http://belajarpsikologi.com/metode-penelitian-kualitatif/

[14] A. Nasir, et, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” vol. 9, pp. 356–363, 2023.

[15] H. Mukminna and D. A. W. Kusumastutie, “Geographic Information Systems for Road Damage Complaints Based on Mobile,” *JTECS J. Sist. Telekomun. Elektron. Sist. Kontrol Power Sist. dan Komput.*, vol. 2, no. 1, p. 55, 2022, doi: 10.32503/jtecs.v2i1.2213.