

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pembahasan

Pada penelitian ini akan dirancang dan dikembangkan sebuah aplikasi yang dapat digunakan untuk mengamankan file dokumen berupa dokumen Word, Excel, dan PDF. Proses pengamanan file dilakukan menggunakan kombinasi algoritma *beaufort cipher* dan hill cipher, yang diterapkan dalam proses enkripsi untuk melindungi file dari akses yang tidak sah. Pengembalian file ke format semula dilakukan melalui proses dekripsi menggunakan algoritma yang sama.

Penggunaan kombinasi algoritma Beaufort Cipher dan Hill Cipher dipilih karena memiliki keunggulan dalam hal kompleksitas keamanan. Beaufort Cipher menawarkan sistem substitusi yang kuat, sementara Hill Cipher menggunakan pendekatan matriks yang memperkuat pengamanan melalui pengolahan data multi-karakter dalam satu operasi. Kombinasi kedua algoritma ini diharapkan mampu meningkatkan keamanan data sekaligus menjaga efisiensi proses enkripsi dan dekripsi.

Aplikasi pada penelitian ini dirancang untuk perangkat mobile dengan sistem operasi Android, sehingga memungkinkan pengguna untuk mengamankan file secara mudah dan fleksibel kapanpun dan di manapun. Untuk memastikan kompatibilitas dan kemudahan penggunaan, antarmuka aplikasi dirancang agar intuitif, dengan fitur utama seperti enkripsi file, dekripsi file, dan manajemen file terenkripsi.

Selain itu, penelitian ini juga mencakup uji coba aplikasi untuk mengukur kinerja algoritma kombinasi dalam berbagai skenario, seperti ukuran file yang berbeda, tipe file, dan kondisi perangkat mobile. Hasil dari uji coba ini akan memberikan evaluasi terhadap efisiensi algoritma, kecepatan proses enkripsi

dan dekripsi, serta tingkat keamanan yang dihasilkan oleh kombinasi algoritma Beaufort Cipher dan Hill Cipher.

Dengan aplikasi ini, diharapkan pengguna dapat memiliki alat yang handal untuk melindungi file-file penting mereka dari ancaman keamanan digital, sekaligus memanfaatkan teknologi mobile untuk kemudahan aksesibilitas dan mobilitas. Penelitian ini juga berkontribusi dalam pengembangan solusi keamanan berbasis algoritma kriptografi pada perangkat mobile.

4.1.1 Analisa Data

Data yang digunakan pada penelitian ini adalah berupa file dokumen yang akan diamankan menggunakan teknik kriptografi dengan kombinasi algoritma beaufort cipher dan hill cipher. Contoh penggunaan dari kombinasi algoritma beaufort cipher dan hill cipher dalam mengamankan file dokumen adalah sebagai berikut :

Contoh : sebuah dokumen word yang memiliki nama file berupa **"dokumen aman"** yang akan di amankan dengan proses enkripsi menggunakan kunci **"siap"**. Proses enkripsi dari file dokumen word tersebut adalah :

1. Proses Enkripsi

Plaintext : dokumen aman

Kunci : siap

Proses enkripsi yang pertama dilakukan adalah menggunakan algoritma beaufort cipher. Pada penelitian ini akan digunakan himpunan 26 karakter dalam proses enkripsi menggunakan algoritma beaufort cipher sehingga didapatkannilai masing-masing karakter adalah :

Tabel 4.1. Himpunan Karakter Algoritma Beaufort Cipher

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nilai	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Karakter	O	P	Q	R	S	T	U	V	W	X	Y	Z		
Nilai	14	15	16	17	18	19	20	21	22	23	24	25		

Proses enkripsi algoritma beaufort cipher adalah sebagai berikut :

$$C1 = (K1 - P1) \bmod 26$$

$$C2 = (K2 - P2) \bmod 26$$

$$\begin{aligned}
 &= (s - d) \bmod 26 \\
 &= (18 - 3) \bmod 26 \\
 &= 15 \\
 &= p
 \end{aligned}$$

$$\begin{aligned}
 C3 &= (K3 - P3) \bmod 26 \\
 &= (a - k) \bmod 26 \\
 &= (0 - 10) \bmod 26 \\
 &= 16 \\
 &= q
 \end{aligned}$$

$$\begin{aligned}
 C5 &= (K5 - P5) \bmod 26 \\
 &= (s - m) \bmod 26 \\
 &= (18 - 12) \bmod 26 \\
 &= 6 \\
 &= g
 \end{aligned}$$

$$\begin{aligned}
 C7 &= (K7 - P7) \bmod 26 \\
 &= (a - n) \bmod 26 \\
 &= (0 - 13) \bmod 26 \\
 &= 13 \\
 &= n
 \end{aligned}$$

$$\begin{aligned}
 C9 &= (K9 - P9) \bmod 26 \\
 &= (s - m) \bmod 26 \\
 &= (18 - 12) \bmod 26 \\
 &= 6 \\
 &= g
 \end{aligned}$$

$$\begin{aligned}
 C11 &= (K11 - P11) \bmod 26 \\
 &= (a - n) \bmod 26 \\
 &= (0 - 13) \bmod 26 \\
 &= 13 \\
 &= n
 \end{aligned}$$

$$\begin{aligned}
 &= (i - o) \bmod 26 \\
 &= (8 - 14) \bmod 26 \\
 &= 20 \\
 &= u
 \end{aligned}$$

$$\begin{aligned}
 C4 &= (K4 - P4) \bmod 26 \\
 &= (p - u) \bmod 26 \\
 &= (15 - 20) \bmod 26 \\
 &= 21 \\
 &= v
 \end{aligned}$$

$$\begin{aligned}
 C6 &= (K6 - P6) \bmod 26 \\
 &= (i - e) \bmod 26 \\
 &= (8 - 4) \bmod 26 \\
 &= 4 \\
 &= e
 \end{aligned}$$

$$\begin{aligned}
 C8 &= (K8 - P8) \bmod 26 \\
 &= (p - a) \bmod 26 \\
 &= (15 - 0) \bmod 26 \\
 &= 15 \\
 &= p
 \end{aligned}$$

$$\begin{aligned}
 C10 &= (K10 - P10) \bmod 26 \\
 &= (i - a) \bmod 26 \\
 &= (8 - 0) \bmod 26 \\
 &= 8 \\
 &= i
 \end{aligned}$$

Hasil dari proses enkripsi menggunakan algoritma beaufort cipher adalah “puqvgenpgin”. Selanjutnya dilakukan proses enkripsi menggunakan algoritma hill cipher terhadap ciphertext yang dihasilkan dari proses enkripsi menggunakan algoritma beaufort cipher. Dalam proses enkripsi menggunakan algoritma hill cipher digunakan urutan himpunan karakter sebagai berikut :

Tabel 4.2. Himpunan Karakter Algoritma Hill Cipher

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nilai	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Karakter	O	P	Q	R	S	T	U	V	W	X	Y	Z	a	b
Nilai	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Karakter	c	d	e	f	g	h	i	j	k	l	m	n	o	p
Nilai	28	29	30	31	32	33	34	35	36	37	38	39	40	41
Karakter	q	r	s	t	u	v	w	x	y	z	0	1	2	3
Nilai	42	43	44	45	46	47	48	49	50	51	52	53	54	55
Karakter	4	5	6	7	8	9		?	!	.	,			
Nilai	56	57	58	59	60	61	62	63	64	65	66			

Plaintext = puqvgenpgin = 41 46 42 47 32 30 39 62 41 32 34 39

Kunci = siap = 44 34 26 41

Proses enkripsi dilakukan dengan cara perhitungan matriks dengan plaintext dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Blok plaintext dienkripsi dengan kunci :

$$C_{1,2} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} \begin{bmatrix} 41 \\ 46 \end{bmatrix} \pmod{67} = \begin{bmatrix} 18 \\ 4 \end{bmatrix} = SE$$

$$C_{3,4} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} \begin{bmatrix} 42 \\ 47 \end{bmatrix} \pmod{67} = \begin{bmatrix} 29 \\ 4 \end{bmatrix} = DE$$

$$C_{5,6} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} \begin{bmatrix} 32 \\ 30 \end{bmatrix} \pmod{67} = \begin{bmatrix} 16 \\ 52 \end{bmatrix} = Q0$$

$$C_{7,8} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} \begin{bmatrix} 39 \\ 62 \end{bmatrix} \pmod{67} = \begin{bmatrix} 5 \\ 5 \end{bmatrix} = FF$$

$$C_{9,10} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} \begin{bmatrix} 41 \\ 32 \end{bmatrix} \pmod{67} = \begin{bmatrix} 11 \\ 33 \end{bmatrix} = Lh$$

$$C_{11,12} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} \begin{bmatrix} 34 \\ 39 \end{bmatrix} \pmod{67} = \begin{bmatrix} 8 \\ 4 \end{bmatrix} = IE$$

Hasil akhir dari proses enkripsi menggunakan kombinasi algoritma

Beaufort dan Hill Cipher adalah “SEDEQ0FFLhIE”.

2. Proses Dekripsi

Proses dekripsi Hill Cipher merupakan tahapan penting dalam mengubah pesan terenkripsi kembali ke dalam bentuk pesan asli. Tahap awal dari proses dekripsi adalah mencari nilai invers dari matriks kunci yang digunakan dalam proses enkripsi. Untuk mendapatkan matriks invers, terdapat dua metode utama yang dapat digunakan, yaitu metode operasi baris (row operation) dan metode determinan. Metode operasi baris melibatkan serangkaian transformasi matematis untuk mengubah matriks kunci menjadi matriks identitas, sementara metode determinan fokus pada perhitungan determinan matriks untuk memastikan matriks dapat diinverskan.

Setelah matriks invers berhasil dihitung, langkah selanjutnya adalah melakukan proses dekripsi sebenarnya. Proses ini dilakukan dengan mengalikan matriks kunci invers dengan blok-blok teks terenkripsi. Setiap blok teks yang telah diproses akan menghasilkan bagian dari pesan asli. Dalam perhitungan ini, operasi modulo digunakan untuk menjaga agar hasil perhitungan tetap berada dalam rentang karakter yang valid. Keberhasilan dekripsi sangat bergantung pada keakuratan perhitungan matriks invers dan pemilihan kunci yang tepat.

Keamanan metode Hill Cipher terletak pada kompleksitas matriks kunci yang digunakan. Matriks kunci harus memiliki determinan yang tidak sama dengan nol, yang berarti matriks tersebut dapat diinverskan. Semakin rumit matriks kunci yang dipilih, semakin sulit pula pesan akan dapat didekripsi oleh pihak yang tidak memiliki kunci yang benar. Proses dekripsi pada dasarnya adalah kebalikan dari proses enkripsi, di mana setiap langkah matematis dirancang untuk mengembalikan pesan ke bentuk aslinya dengan presisi yang tinggi.

Menariknya, Hill Cipher merupakan salah satu metode enkripsi klasik yang menggunakan aljabar linier dalam proses pengamanannya. Berbeda dengan metode substitusi sederhana, Hill Cipher mampu mengenkripsi

beberapa huruf sekaligus dalam satu blok, yang membuatnya lebih sulit untuk dipecahkan menggunakan analisis frekuensi tradisional. Namun, kelemahan utama metode ini adalah kerentanannya terhadap serangan matematika yang canggih jika kunci tidak dipilih dengan hati-hati. Setelah melakukan perhitungan, didapat matriks K^{-1} yang merupakan invers dari matriks K, yaitu:

$$K^{-1} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} = \begin{bmatrix} 44 & 34 \\ 26 & 41 \end{bmatrix} (\text{mod } 67)$$

Sehingga di dapatkan nilai kunci invers yang akan digunakan dalam proses dekripsi menggunakan algoritma hill cipher adalah -6 54 61 -62. Selanjutnya dilakukan proses dekripsi menggunakan algoritma Hill Cipher sebagai berikut :

$$C_{1,2} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 18 \\ 4 \end{bmatrix} (\text{mod } 67) = \begin{bmatrix} 41 \\ 46 \end{bmatrix} = \text{pu}$$

$$C_{3,4} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 29 \\ 4 \end{bmatrix} (\text{mod } 67) = \begin{bmatrix} 42 \\ 47 \end{bmatrix} = \text{qv}$$

$$C_{5,6} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 16 \\ 52 \end{bmatrix} (\text{mod } 67) = \begin{bmatrix} 32 \\ 30 \end{bmatrix} = \text{ge}$$

$$C_{7,8} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} (\text{mod } 67) = \begin{bmatrix} 39 \\ 62 \end{bmatrix} = \text{n}$$

$$C_{9,10} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 11 \\ 33 \end{bmatrix} (\text{mod } 67) = \begin{bmatrix} 41 \\ 32 \end{bmatrix} = \text{pg}$$

$$C_{11,12} = \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 8 \\ 4 \end{bmatrix} (\text{mod } 67) = \begin{bmatrix} 34 \\ 39 \end{bmatrix} = \text{in}$$

Hasil dekripsi yang di dapat menggunakan algoritma Hill Cipher adalah **“puqvgen pgin”**. Selanjutnya dilakukan kembali proses dekripsi menggunakan algoritma Beaufort sebagai berikut :

Plaintext : puqvgen pgin

Kunci : siap

$$P1 = (K1 - C1) \text{ mod } 26$$

$$= (s - p) \text{ mod } 26$$

$$= (18 - 15) \text{ mod } 26$$

$$= 3$$

$$= d$$

$$P2 = (K2 - C2) \text{ mod } 26$$

$$= (i - u) \text{ mod } 26$$

$$= (8 - 20) \text{ mod } 26$$

$$= 14$$

$$= o$$

$$\begin{aligned}
 P3 &= (K3 - C3) \bmod 26 \\
 &= (a - q) \bmod 26 \\
 &= (0 - 16) \bmod 26 \\
 &= 10 \\
 &= k
 \end{aligned}$$

$$\begin{aligned}
 P5 &= (K5 - C5) \bmod 26 \\
 &= (s - g) \bmod 26 \\
 &= (18 - 6) \bmod 26 \\
 &= 12 \\
 &= m
 \end{aligned}$$

$$\begin{aligned}
 P7 &= (K7 - C7) \bmod 26 \\
 &= (a - n) \bmod 26 \\
 &= (0 - 13) \bmod 26 \\
 &= 13 \\
 &= n
 \end{aligned}$$

$$\begin{aligned}
 P9 &= (K9 - C9) \bmod 26 \\
 &= (s - g) \bmod 26 \\
 &= (18 - 6) \bmod 26 \\
 &= 12 \\
 &= m
 \end{aligned}$$

$$\begin{aligned}
 P11 &= (K11 - C11) \bmod 26 \\
 &= (a - n) \bmod 26 \\
 &= (0 - 13) \bmod 26 \\
 &= 13 \\
 &= n
 \end{aligned}$$

$$\begin{aligned}
 P4 &= (K4 - C4) \bmod 26 \\
 &= (p - v) \bmod 26 \\
 &= (15 - 21) \bmod 26 \\
 &= 20 \\
 &= u
 \end{aligned}$$

$$\begin{aligned}
 P6 &= (K6 - C6) \bmod 26 \\
 &= (i - e) \bmod 26 \\
 &= (8 - 4) \bmod 26 \\
 &= 4 \\
 &= e
 \end{aligned}$$

$$\begin{aligned}
 P8 &= (K8 - C8) \bmod 26 \\
 &= (p - p) \bmod 26 \\
 &= (15 - 15) \bmod 26 \\
 &= 0 \\
 &= a
 \end{aligned}$$

$$\begin{aligned}
 P10 &= (K10 - C10) \bmod 26 \\
 &= (i - i) \bmod 26 \\
 &= (8 - 8) \bmod 26 \\
 &= 0 \\
 &= a
 \end{aligned}$$

Dari proses dekripsi menggunakan algoritma Beaufort di dapatkan hasil akhir *plaintext* berupa “**dokumen aman**”.

4.1.2 Flowchart Sistem

4.1.2.1 Flowchart Menu Enkripsi Dokumen

Flowchart Menu Enkripsi Dokumen merupakan representasi visual yang komprehensif dari proses sistematis enkripsi dokumen dalam aplikasi. Diagram alur ini menggambarkan serangkaian langkah terstruktur yang dilalui pengguna ketika hendak mengenkripsi berbagai jenis dokumen seperti Word, Excel, dan PDF. Tujuan utama dari flowchart ini adalah menjelaskan alur kerja yang logis dan sekuensial dalam proses keamanan dokumen.

Proses enkripsi dokumen umumnya dimulai dari tahap awal yaitu pengguna memilih menu enkripsi dalam aplikasi. Tahap selanjutnya melibatkan pemilihan tipe dokumen yang akan dienkripsi - apakah dokumen Microsoft Word, Microsoft Excel, atau dokumen PDF. Setiap jenis dokumen memiliki karakteristik format dan struktur data yang berbeda, sehingga proses enkripsi harus disesuaikan dengan tipe dokumen tersebut.

Setelah memilih tipe dokumen, pengguna akan diarahkan untuk memilih file spesifik yang ingin dienkripsi. Proses seleksi file ini biasanya melibatkan dialog standar sistem operasi yang memungkinkan pengguna menelusuri direktori penyimpanan dokumen. Kemudian, pengguna akan diminta untuk memasukkan kunci enkripsi - sebuah langkah kritis yang akan menentukan keamanan dokumen.

Algoritma enkripsi yang digunakan, dalam konteks ini menggunakan Hill Cipher, akan memproses dokumen dengan mengubah konten menjadi format terenkripsi. Proses ini melibatkan serangkaian perhitungan matematis kompleks yang mentransformasikan data dokumen menjadi bentuk yang tidak dapat dibaca tanpa kunci dekripsi yang benar. Algoritma akan mengenkripsi data blok per blok, memastikan keseluruhan konten dokumen terproteksi.

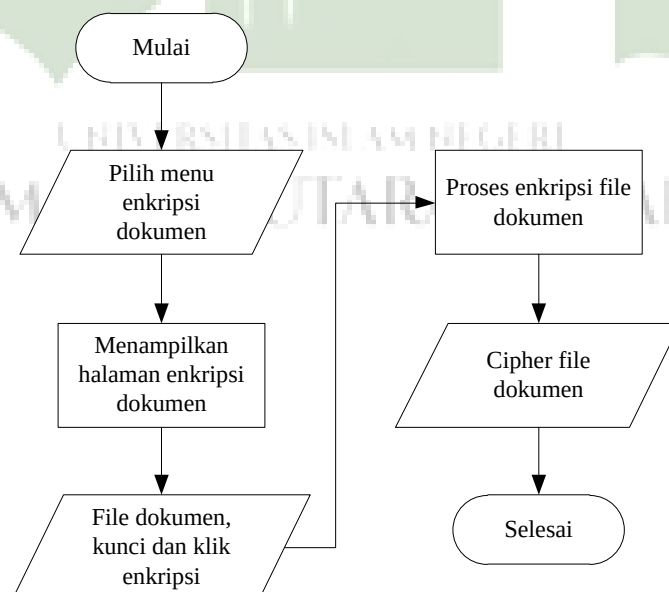
Setelah proses enkripsi selesai dilakukan, flowchart biasanya menunjukkan tahap penyimpanan dokumen terenkripsi. Pengguna dapat memilih lokasi penyimpanan dokumen yang telah dienkripsi, dengan aplikasi memberikan konfirmasi bahwa proses enkripsi telah berhasil diselesaikan.

Beberapa implementasi mungkin juga menyertakan opsi untuk menghapus dokumen asli atau membuat salinan terenkripsi.

Poin penting dalam flowchart menu enkripsi dokumen adalah memastikan keamanan dan kemudahan penggunaan secara simultan. Desain alur kerja harus intuitif bagi pengguna awam namun memiliki mekanisme keamanan yang kuat. Hal ini mencakup validasi input kunci, penanganan error, dan memastikan tidak ada kebocoran data selama proses enkripsi berlangsung.

Kompleksitas flowchart juga mencerminkan tantangan teknis dalam mengenkripsi berbagai format dokumen. Setiap tipe dokumen - Word, Excel, PDF - memiliki struktur internal yang berbeda, yang memerlukan pendekatan khusus dalam proses enkripsi. Algoritma Hill Cipher harus mampu beradaptasi dengan variasi format ini tanpa merusak integritas dokumen asli.

Terakhir, flowchart menu enkripsi dokumen bukan sekadar diagram teknis, melainkan representasi filosofis tentang perlindungan informasi di era digital. Setiap langkah dalam diagram menggambarkan upaya sistematis untuk mengamankan data sensitif dari akses yang tidak sah, mencerminkan pentingnya kerahasiaan informasi dalam konteks teknologi modern. Flowchart menu enkripsi dokumen dapat dilihat pada gambar 4.1.



Gambar 4.1. Flowchart Menu Enkripsi Dokumen

4.1.2.2 Flowchart Menu Dekripsi Dokumen

Flowchart Menu Dekripsi Dokumen merupakan representasi sistematis dari proses pengembalian dokumen terenkripsi ke dalam bentuk asli dan dapat dibaca. Diagram alur ini menggambarkan serangkaian langkah yang harus dilalui pengguna untuk mendapatkan kembali dokumen yang sebelumnya telah dienkripsi menggunakan algoritma tertentu, dalam konteks ini menggunakan Hill Cipher.

Proses dekripsi dimulai dari tahap awal yaitu pengguna memilih menu dekripsi dalam aplikasi. Tahap ini merupakan titik awal yang kritis, di mana pengguna mengindikasikan intensi untuk membuka kembali dokumen yang telah diamankan. Berbeda dengan proses enkripsi, dekripsi membutuhkan kecocokan kunci yang tepat untuk dapat membuka dokumen.

Setelah memilih menu dekripsi, pengguna akan diarahkan untuk memilih file terenkripsi yang ingin didekripsi. Proses seleksi file ini biasanya melibatkan dialog sistem operasi yang memungkinkan pengguna menelusuri direktori penyimpanan dokumen terenkripsi. Tahap ini penting karena hanya dokumen dengan format terenkripsi yang dapat diproses lebih lanjut.

Langkah selanjutnya adalah memasukkan kunci dekripsi. Kunci ini harus identik dengan kunci yang digunakan pada saat proses enkripsi awal. Kecocokan kunci menjadi syarat mutlak keberhasilan dekripsi. Jika kunci yang dimasukkan salah, proses dekripsi akan gagal, dan dokumen tidak dapat dikembalikan ke bentuk aslinya. Hal ini merupakan mekanisme keamanan yang fundamental dalam sistem enkripsi.

Algoritma Hill Cipher yang digunakan akan memproses dokumen terenkripsi dengan serangkaian perhitungan matematis kompleks. Proses ini melibatkan penggunaan matriks invers kunci untuk mentransformasi data terenkripsi kembali ke bentuk asli. Setiap blok data akan diproses secara berurutan, memastikan keseluruhan konten dokumen dapat dikembalikan dengan presisi.

Sistem akan melakukan validasi terhadap kunci dan proses dekripsi. Jika kunci valid dan proses berhasil, dokumen akan dikembalikan ke format

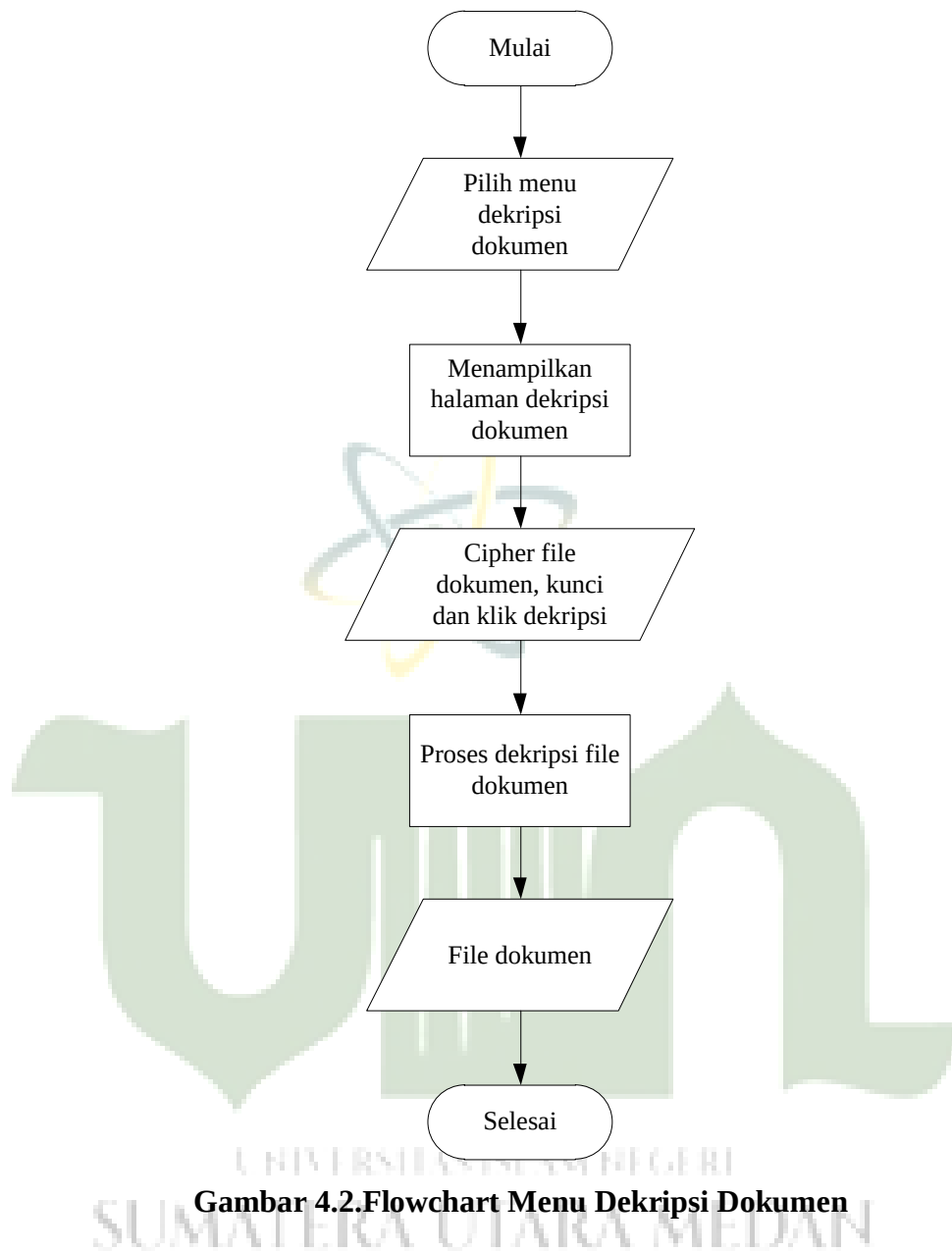
aslinya - baik itu dokumen Word, Excel, atau PDF. Beberapa implementasi mungkin menyertakan opsi untuk menyimpan dokumen yang sudah didekripsi di lokasi baru, memberikan fleksibilitas kepada pengguna.

Aspek penting lainnya dalam flowchart dekripsi dokumen adalah penanganan potensi kesalahan. Sistem harus mampu memberikan umpan balik yang jelas kepada pengguna jika terjadi kegagalan dekripsi, baik karena kesalahan kunci, kerusakan file, atau masalah kompatibilitas format. Komunikasi yang transparan tentang status proses sangat penting untuk pengalaman pengguna.

Kompleksitas flowchart mencerminkan tantangan teknis dalam mendekripsi berbagai format dokumen. Setiap tipe dokumen memiliki struktur internal unik, yang memerlukan pendekatan presisi dalam proses dekripsi. Algoritma Hill Cipher harus mampu mengembalikan dokumen ke kondisi persis seperti sebelum dienkripsi, tanpa kehilangan atau merusak data.

Secara filosofis, flowchart menu dekripsi dokumen menggambarkan konsep keamanan yang seimbang. Di satu sisi, proses dekripsi memberikan mekanisme untuk membuka kembali informasi yang telah diamankan, namun di sisi lain, tetap mempertahankan kendali akses melalui mekanisme kunci yang ketat. Ini mencerminkan keseimbangan antara perlindungan data dan aksesibilitas informasi di era digital.

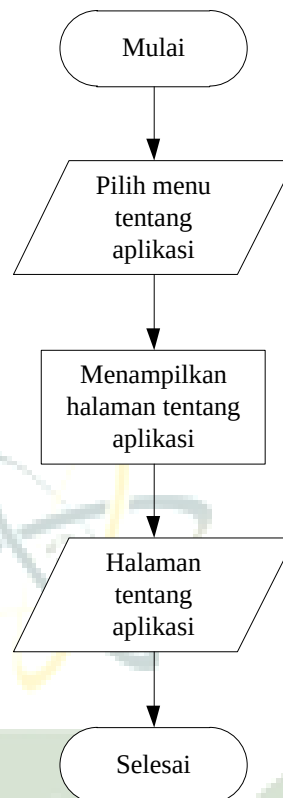
Flowchart bukan sekadar diagram teknis, melainkan representasi kompleksitas perlindungan informasi. Setiap langkah menunjukkan upaya sistematis untuk memastikan bahwa hanya pihak yang berwenang dapat mengakses dokumen. Flowchart menu dekripsi dokumen dapat dilihat pada gambar 4.2.



Gambar 4.2. Flowchart Menu Dekripsi Dokumen

4.1.2.3 Flowchart Menu Tentang Aplikasi

Flowchart menu tentang aplikasi menggambarkan alur penggunaan aplikasi dalam menampilkan halaman tentang aplikasi. Flowchart menu tentang aplikasi dapat dilihat pada gambar 4.3.



Gambar 4.3. Flowchart Menu Tentang Aplikasi

Flowchart Menu Tentang Aplikasi merupakan representasi visual yang menggambarkan alur navigasi pengguna menuju halaman informasi dasar tentang aplikasi enkripsi dokumen. Diagram alur ini menjelaskan proses sederhana namun penting dalam memberikan transparansi dan pemahaman kepada pengguna tentang latar belakang, tujuan, dan karakteristik aplikasi yang mereka gunakan.

Proses dimulai ketika pengguna memilih menu "Tentang" atau "About" dalam antarmuka aplikasi. Ini merupakan titik awal interaksi pengguna dengan informasi meta-aplikasi, yang biasanya dapat diakses melalui menu utama atau ikon informasi. Pemilihan menu ini mengindikasikan ketertarikan pengguna untuk memahami lebih dalam tentang aplikasi yang sedang mereka gunakan.

Setelah memilih menu, sistem akan secara otomatis mengarahkan pengguna ke halaman khusus yang berisi informasi komprehensif tentang

aplikasi. Halaman ini umumnya mencakup beberapa komponen kunci yang memberikan wawasan mendalam tentang aplikasi enkripsi dokumen. Informasi yang biasanya disertakan meliputi deskripsi singkat fungsionalitas aplikasi, tujuan pengembangan, versi perangkat lunak, dan fitur utama yang ditawarkan.

Aspek penting dalam halaman "Tentang Aplikasi" adalah penjelasan tentang metodologi keamanan yang digunakan. Dalam konteks aplikasi enkripsi dokumen ini, halaman akan menjelaskan penggunaan algoritma Hill Cipher, prinsip kerja enkripsi dan dekripsi, serta keunggulan metode ini dalam melindungi dokumen sensitif. Ini membantu pengguna memahami mekanisme keamanan yang mendasari aplikasi.

Informasi tambahan yang umumnya disertakan mencakup detail pengembang, tanggal rilis, versi aplikasi, dan catatan perubahan (changelog). Beberapa aplikasi juga mencantumkan informasi lisensi, persyaratan penggunaan, serta kredit untuk pustaka atau teknologi pihak ketiga yang digunakan dalam pengembangan. Hal ini memberikan transparansi dan kredibilitas kepada pengguna.

Flowchart menggambarkan bahwa setelah menampilkan informasi, pengguna memiliki opsi untuk kembali ke menu utama. Ini mencerminkan desain antarmuka yang intuitif dan memudahkan navigasi. Kemudahan akses dan kemampuan untuk dengan cepat kembali ke fungsi utama aplikasi adalah prinsip desain yang penting dalam pengembangan perangkat lunak modern. Secara filosofis, halaman "Tentang Aplikasi" lebih dari sekadar kumpulan informasi teknis. Ini adalah jendela yang memperlihatkan visi dan misi di balik pengembangan aplikasi. Bagi pengguna yang peduli dengan keamanan digital, halaman ini memberikan keyakinan tentang keseriusan dan profesionalisme tim pengembang dalam menciptakan solusi perlindungan data.

Desain flowchart menu tentang aplikasi mencerminkan pendekatan user-centric dalam pengembangan perangkat lunak. Setiap elemen dirancang untuk memberikan pengalaman yang transparan, informatif, dan mudah

dinavigasi. Ini tidak hanya tentang memberikan informasi, tetapi juga tentang membangun kepercayaan pengguna melalui keterbukaan dan kejelasan.

Terakhir, flowchart ini menggambarkan bahwa halaman "Tentang Aplikasi" adalah titik kontak penting antara pengembang dan pengguna. Ini adalah ruang di mana teknologi bertemu dengan narasi manusia, di mana fungsi teknis disambungkan dengan maksud dan tujuan penciptaan aplikasi dalam konteks keamanan informasi digital kontemporer.

Dengan demikian, flowchart menu tentang aplikasi tidak sekadar menggambarkan alur navigasi, tetapi juga menceritakan filosofi di balik penciptaan sebuah solusi teknologi yang bertujuan melindungi dan memberdayakan pengguna dalam mengelola dokumen sensitif mereka.

4.1.3 Desain Antarmuka

Desain halaman utama pada aplikasi pengamanan dokumen berbasis mobile merupakan tampilan pertama yang akan dilihat pengguna saat membuka aplikasi. Halaman ini memiliki peran penting dalam memberikan kesan awal dan memperkenalkan fungsi-fungsi utama aplikasi kepada pengguna.

Secara visual, halaman utama dirancang dengan tampilan sederhana namun informatif. Tata letak antarmuka dibuat agar mudah dipahami oleh berbagai kalangan pengguna, mulai dari pemula hingga pengguna berpengalaman. Desain memperhatikan kemudahan navigasi dan kejelasan setiap menu yang tersedia.

Menu utama pada halaman berisi pilihan-pilihan dasar yang dibutuhkan pengguna dalam mengamankan dokumen. Kemungkinan menu yang tersedia mencakup enkripsi dokumen, dekripsi dokumen, pengaturan aplikasi, dan informasi tentang aplikasi. Setiap menu dilengkapi dengan ikon yang menjelaskan fungsinya, sehingga pengguna dapat dengan cepat memahami cara kerja aplikasi.

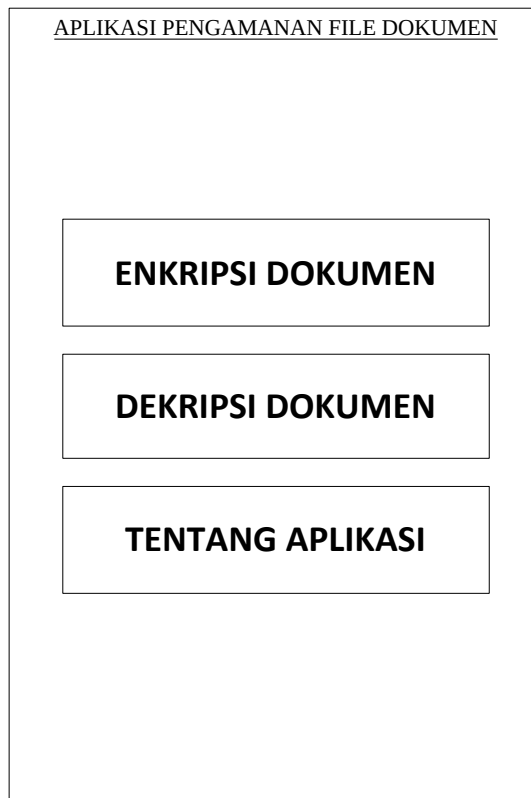
Pemilihan warna dan desain visual dirancang untuk menciptakan kesan aman dan terpercaya. Penggunaan warna-warna netral seperti biru atau abu-abu memberikan nuansa profesional dan menenangkan. Desain minimalis membantu pengguna fokus pada tugas utama mengamankan dokumen tanpa gangguan visual yang berlebihan.

Pertimbangan khusus diberikan pada desain antarmuka mobile, mengingat keterbatasan layar perangkat telepon pintar. Setiap elemen dirancang agar mudah dipilih dengan sentuhan jari, tidak terlalu kecil, dan tidak membuat layar terlihat padat. Tujuannya adalah menciptakan pengalaman pengguna yang nyaman dan intuitif.

Halaman utama berfungsi sebagai pusat kendali aplikasi. Pengguna dapat dengan mudah memilih fungsi yang diinginkan, seperti mengenkripsi dokumen baru, mendekripsi dokumen yang telah diamankan, atau mengakses pengaturan lanjutan. Desain memastikan setiap tindakan dapat dilakukan dengan cepat dan mudah.

Keamanan tidak hanya tercermin dalam fitur teknis, tetapi juga dalam desain antarmuka. Tampilan yang profesional dan bersih memberikan kepercayaan kepada pengguna bahwa aplikasi serius dalam melindungi dokumen mereka. Penggunaan ikon kunci dan tata letak yang rapi menguatkan kesan keamanan.

Halaman utama adalah jendela pertama yang menghubungkan pengguna dengan solusi pengamanan dokumen. Desain yang cermat memadukan estetika, fungsionalitas, dan kemudahan penggunaan untuk menciptakan pengalaman yang memberdayakan pengguna dalam melindungi informasi penting mereka di era digital. Desain halaman utama dapat dilihat pada gambar 4.4.



Gambar 4.4. Desain Halaman Utama

1. Desain Halaman Enkripsi Dokumen

Desain halaman enkripsi dokumen merupakan elemen kritis dalam aplikasi pengamanan dokumen, dirancang untuk memungkinkan pengguna melakukan proses enkripsi secara efektif pada berbagai jenis dokumen seperti Word, Excel, dan PDF. Dengan pendekatan desain yang mengutamakan kemudahan penggunaan dan keamanan, halaman ini menjadi solusi yang tepat untuk melindungi data sensitif dari ancaman pihak tidak bertanggung jawab.

Secara fungsional, halaman enkripsi dirancang untuk memberikan pengalaman pengguna yang lancar dan intuitif. Pengguna dapat dengan mudah memilih file dokumen melalui dialog standar sistem operasi mobile. Antarmuka ini memungkinkan pengguna untuk menelusuri dan memilih dokumen dari penyimpanan perangkat tanpa hambatan. Langkah ini memastikan kompatibilitas yang luas dengan berbagai jenis perangkat dan

sistem operasi, menjadikan proses pengamanan dokumen lebih inklusif. Salah satu fitur utama yang menonjol adalah batasan penggunaan kunci enkripsi. Sistem hanya mengizinkan penggunaan empat karakter huruf dengan rentang karakter terbatas dari “a” hingga “x”. Pembatasan ini bukan sekadar keputusan teknis, melainkan didasarkan pada karakteristik algoritma enkripsi yang digunakan, yaitu Beaufort Cipher dan batasan komputasi matriks pada Hill Cipher. Dengan demikian, pembatasan ini memastikan algoritma bekerja secara optimal dan tetap aman. Desain antarmuka pengisian kunci dirancang sederhana namun sangat terkontrol. Kotak input kunci dilengkapi dengan validasi otomatis yang mencegah pengguna memasukkan karakter selain huruf atau melebihi empat karakter. Validasi ini tidak hanya mencegah kesalahan input, tetapi juga memastikan kepatuhan terhadap persyaratan algoritma enkripsi. Dengan demikian, proses enkripsi dapat dilakukan dengan lebih cepat dan tanpa hambatan teknis. Tombol enkripsi ditempatkan secara strategis untuk memberikan akses langsung ke proses pengamanan dokumen.

Setelah pengguna memilih file dan memasukkan kunci, mereka dapat dengan mudah memulai proses enkripsi hanya dengan sekali sentuh. Desain tombol dibuat mencolok dan intuitif, mengikuti prinsip desain antarmuka mobile yang baik. Hal ini memastikan pengguna, baik dari kalangan profesional maupun pengguna awam, dapat mengoperasikan fitur ini dengan mudah. Pembatasan panjang dan jenis karakter kunci, meskipun terlihat sederhana, merupakan strategi keamanan yang cerdas. Semakin pendek dan terbatasnya kunci, semakin sulit bagi pihak jahat untuk melakukan serangan brute force. Selain itu, implementasi algoritma seperti Beaufort Cipher dan Hill Cipher memberikan lapisan keamanan tambahan, membuat proses enkripsi lebih tahan terhadap berbagai jenis serangan kriptografi. Fleksibilitas aplikasi ini tercermin dari kemampuannya mengenkripsi berbagai format dokumen, termasuk Word, Excel, dan PDF. Dengan menyediakan dukungan multi-format dalam satu antarmuka, aplikasi ini memudahkan pengguna yang bekerja dengan berbagai jenis dokumen. Hal ini menunjukkan pendekatan

komprehensif dalam memenuhi kebutuhan perlindungan data pengguna yang beragam. Halaman enkripsi dokumen dirancang dengan mengikuti prinsip desain modern, seperti penggunaan elemen visual yang bersih dan tata letak yang responsif. Setiap elemen dirancang untuk memudahkan navigasi, meningkatkan pengalaman pengguna, dan mempercepat proses enkripsi. Selain itu, desain responsif memastikan halaman tetap berfungsi optimal pada berbagai ukuran layar perangkat. Desain halaman enkripsi bukan sekadar antarmuka teknis, melainkan titik pertemuan antara teknologi keamanan canggih dan kebutuhan praktis pengguna. Setiap elemen, mulai dari antarmuka pemilihan dokumen hingga tombol enkripsi, dirancang untuk membuat proses pengamanan dokumen menjadi sederhana, aman, dan mudah diakses. Dengan fokus pada keamanan dan kemudahan penggunaan, halaman ini memberikan solusi menyeluruh untuk pengamanan data dalam berbagai situasi. Desain halaman enkripsi dokumen menawarkan kombinasi yang seimbang antara keamanan, fleksibilitas, dan kemudahan penggunaan. Dengan antarmuka yang intuitif, validasi input yang ketat, serta dukungan multi-format dokumen, aplikasi ini menjadi alat yang efektif untuk melindungi dokumen penting. Desainnya mencerminkan komitmen terhadap kebutuhan pengguna modern yang mengutamakan keamanan data tanpa mengorbankan kenyamanan. Halaman ini menjadi bukti bahwa teknologi keamanan dapat diimplementasikan dengan cara yang inklusif dan praktis. Desain halaman enkripsi dokumen dapat dilihat pada gambar 4.5.

SUMATERA UTARA MEDAN

The image shows a web application interface for file encryption. It consists of a main container with a title 'ENKRIPSI FILE DOKUMEN'. Below the title, there are four distinct components arranged vertically: a button labeled 'File dokumen...', a button labeled 'PILIH DOKUMEN', a text input field labeled 'Input kunci..', and a button labeled 'ENKRIPSI'.

Gambar 4.5. Desain Halaman Enkripsi File Dokumen

2. Desain Halaman Dekripsi Dokumen

Halaman dekripsi dokumen dirancang untuk mempermudah pengguna dalam memulihkan dokumen yang telah dienkripsi sebelumnya ke bentuk aslinya. Proses ini sangat penting untuk memastikan data tetap dapat diakses hanya oleh pihak yang berwenang. Antarmuka halaman ini dirancang dengan prinsip yang sederhana dan intuitif agar pengguna dapat menjalankan proses dekripsi tanpa kesulitan. Validasi kunci sangat ditekankan untuk memastikan bahwa hanya kunci yang sesuai dengan proses enkripsi awal yang dapat digunakan, sehingga menjaga keamanan data. Tombol dekripsi ditempatkan secara strategis untuk memberikan akses mudah kepada pengguna dalam menjalankan fungsi utama ini. Dengan mengintegrasikan algoritma Beaufort Cipher dan Hill Cipher, halaman dekripsi memberikan jaminan keamanan yang tinggi dalam

prosesnya. Desain ini tidak hanya berfokus pada keamanan teknis tetapi juga pada kemudahan penggunaan, memastikan bahwa baik pengguna profesional maupun awam dapat mengoperasikan fitur ini dengan efisien. Penambahan elemen visual seperti gambar panduan, seperti yang ditunjukkan pada Gambar 4.6, membantu memberikan pemahaman yang lebih jelas kepada pengguna tentang alur kerja halaman ini. Kombinasi dari pendekatan keamanan, kejelasan antarmuka, dan dukungan algoritma kriptografi membuat halaman ini menjadi komponen penting dalam sistem pengamanan dokumen secara menyeluruh. Desain halaman dekripsi dokumen dapat dilihat pada gambar 4.6.



The image shows a web form for document decryption. It has a title bar at the top that says "DEKRIPSI FILE DOKUMEN". Below the title bar, there are four distinct rectangular boxes stacked vertically. The first box contains the text "File dokumen...". The second box contains the text "PILIH CIPHER DOKUMEN". The third box contains the text "Input kunci..". The fourth box contains the text "DEKRIPSI". The background of the page is white with a faint green watermark on the left side that says "SUMA" and "AN".

Gambar 4.6. Desain Halaman Dekripsi Dokumen

3. Desain Halaman Tentang Aplikasi

Desain halaman tentang aplikasi memiliki peran penting dalam memberikan transparansi dan informasi mendalam kepada pengguna tentang latar belakang dan tujuan pengembangan aplikasi keamanan

dokumen. Halaman ini dirancang untuk menampilkan informasi kunci tentang penelitian, peneliti, dan filosofi di balik penciptaan aplikasi.

Secara visual, halaman ini mengutamakan kesederhanaan dan kejelasan informasi. Logo Universitas Islam Negeri Sumatera Utara ditempatkan secara prominens, memberikan legitimasi akademis dan institusional terhadap pengembangan aplikasi. Penggunaan logo institusi pendidikan menandakan bahwa aplikasi ini lahir dari proses penelitian ilmiah yang terstruktur dan terarah.

Informasi personal peneliti disajikan dengan jelas dan transparan. Nama lengkap Muhaimi Rizki Siregar dan Nomor Induk Mahasiswa (NIM) 0701173195 dicantumkan untuk memberikan kredibilitas dan akuntabilitas. Hal ini mencerminkan praktik ilmiah yang menjunjung tinggi keterbukaan dan pengakuan kontribusi individual dalam pengembangan teknologi.

Judul penelitian "Kombinasi Algoritma Beaufort Cipher Dan Hill Cipher Dalam Mengamankan File Dokumen Berbasis Mobile" menjadi focal point halaman. Judul tersebut tidak hanya sekadar informasi administratif, melainkan menjelaskan filosofi dan pendekatan inovatif dalam merancang solusi keamanan dokumen. Gagasan mengombinasikan dua algoritma berbeda menunjukkan upaya untuk meningkatkan kompleksitas dan efektivitas pengamanan data.

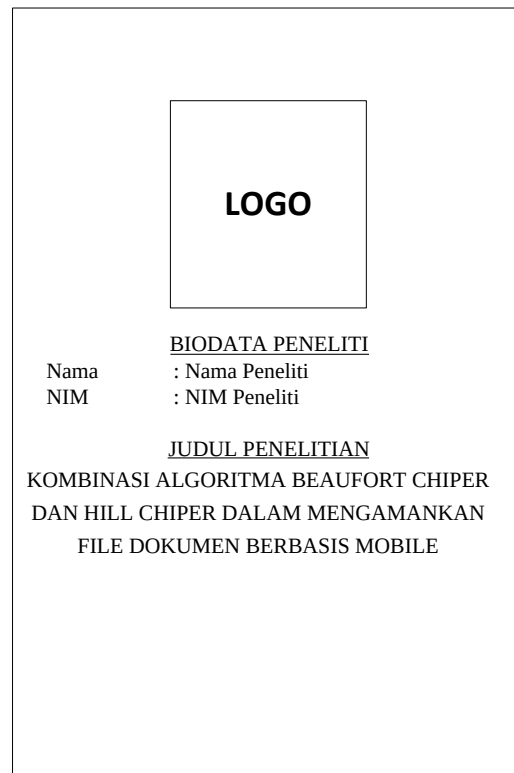
Konsep kombinasi algoritma Beaufort Cipher dan Hill Cipher merupakan strategi cerdas dalam mengembangkan sistem keamanan. Dengan menggabungkan dua metodologi enkripsi yang berbeda, peneliti berupaya menciptakan lapisan keamanan ganda. Pendekatan ini lebih unggul dibandingkan penggunaan algoritma tunggal, karena meningkatkan kompleksitas proses enkripsi dan menurunkan potensi celah keamanan.

Desain antarmuka halaman tentang dibangun dengan mempertimbangkan aspek estetika dan keterbacaan. Pemilihan tipografi, warna, dan tata letak dirancang untuk memudahkan pengguna memahami informasi dengan cepat. Elemen-elemen visual disusun secara hierarkis, membimbing mata pembaca untuk memahami informasi secara sistematis.

Halaman ini juga berfungsi sebagai medium komunikasi antara peneliti dan pengguna. Selain memberikan informasi faktual, desain halaman menciptakan narasi tentang motivasi di balik pengembangan aplikasi. Penekanan pada kombinasi algoritma menggambarkan semangat inovasi dan komitmen untuk terus mengembangkan solusi keamanan informasi yang lebih canggih.

Secara akademis, halaman tentang aplikasi mendokumentasikan proses penelitian dan pengembangan. Ia menjadi bukti nyata bahwa aplikasi ini bukan sekadar produk teknologi, melainkan hasil riset mendalam yang mempertimbangkan aspek teoritis dan praktis pengamanan dokumen digital.

Desain halaman tentang aplikasi mencerminkan nilai-nilai transparansi, inovasi, dan dedikasi dalam pengembangan teknologi keamanan informasi. Setiap elemen dirancang untuk tidak hanya menginformasikan, tetapi juga menginspirasi dan membangun kepercayaan pengguna terhadap solusi keamanan dokumen yang dihadirkan..Desain halaman tentang aplikasi dapat dilihat pada gambar 4.7.



Gambar 4.7. Desain Halaman Tentang Aplikasi

4.2 Hasil

Pada penelitian ini telah dihasilkan sebuah aplikasi yang dapat digunakan untuk mengamankan file dokumen word, dokumen excel dan dokumen PDF menggunakan kombinasi algoritma beaufort cipher dan hill cipher.

4.2.1 Pengujian Aplikasi

Halaman utama aplikasi pengamanan dokumen merupakan antarmuka pertama yang dihadapi pengguna saat membuka aplikasi pada perangkat mobile. Desain halaman ini memiliki peran strategis dalam memberikan gambaran awal tentang fungsi dan kemudahan penggunaan aplikasi keamanan dokumen yang dikembangkan.

Berdasarkan hasil penelitian, halaman utama dirancang secara sederhana namun informatif dengan menampilkan tiga menu utama. Ketiga menu tersebut mencakup enkripsi dokumen, dekripsi dokumen, dan informasi tentang aplikasi. Setiap menu dilengkapi dengan ikon yang representatif, memudahkan pengguna

untuk memahami fungsi masing-masing fitur tanpa mengalami kesulitan navigasi.

Pertimbangan utama dalam merancang antarmuka mobile adalah kemudahan akses dan keterbacaan. Oleh karena itu, desain halaman utama memperhatikan aspek tata letak yang proporsional, dengan memberikan ruang yang cukup di antara setiap ikon. Hal ini memastikan pengguna dapat dengan mudah memilih menu yang diinginkan, bahkan pada perangkat dengan layar berukuran terbatas.

Pemilihan warna dan gaya visual tidak dilakukan secara acak, melainkan melalui pertimbangan mendalam untuk menciptakan kesan profesional dan terpercaya. Warna-warna netral yang dipilih bertujuan memberikan nuansa keamanan, sementara tipografi yang digunakan dirancang agar mudah dibaca dan dipahami oleh berbagai kalangan pengguna.

Secara fungsional, halaman utama bertindak sebagai pusat kendali aplikasi. Pengguna dapat langsung mengakses fitur enkripsi untuk mengamankan dokumen, melakukan dekripsi untuk membuka dokumen yang telah diamankan, atau melihat informasi detail tentang aplikasi. Desain yang intuitif ini memungkinkan pengguna dari berbagai latar belakang untuk segera mulai menggunakan aplikasi tanpa mengalami kesulitan.

Konsep desain halaman utama tidak sekadar memperhatikan aspek teknis, tetapi juga mempertimbangkan pengalaman pengguna secara menyeluruh. Setiap elemen visual dirancang untuk menciptakan alur interaksi yang lancar, aman, dan memberikan rasa nyaman kepada pengguna dalam melindungi dokumen sensitif mereka.

Dengan demikian, halaman utama aplikasi tidak hanya berfungsi sebagai pintu masuk, tetapi juga menjadi cermin filosofi pengembangan aplikasi. Desain yang sederhana namun cerdas ini mencerminkan komitmen peneliti dalam menciptakan solusi keamanan dokumen yang mudah digunakan, dapat dipercaya, dan memenuhi kebutuhan pengguna di era digital saat ini. Halaman utama dari aplikasi dapat dilihat pada gambar 4.8 sebagai berikut :



Gambar 4.8. Tampilan Halaman Utama

1. Tampilan Halaman Enkripsi Dokumen

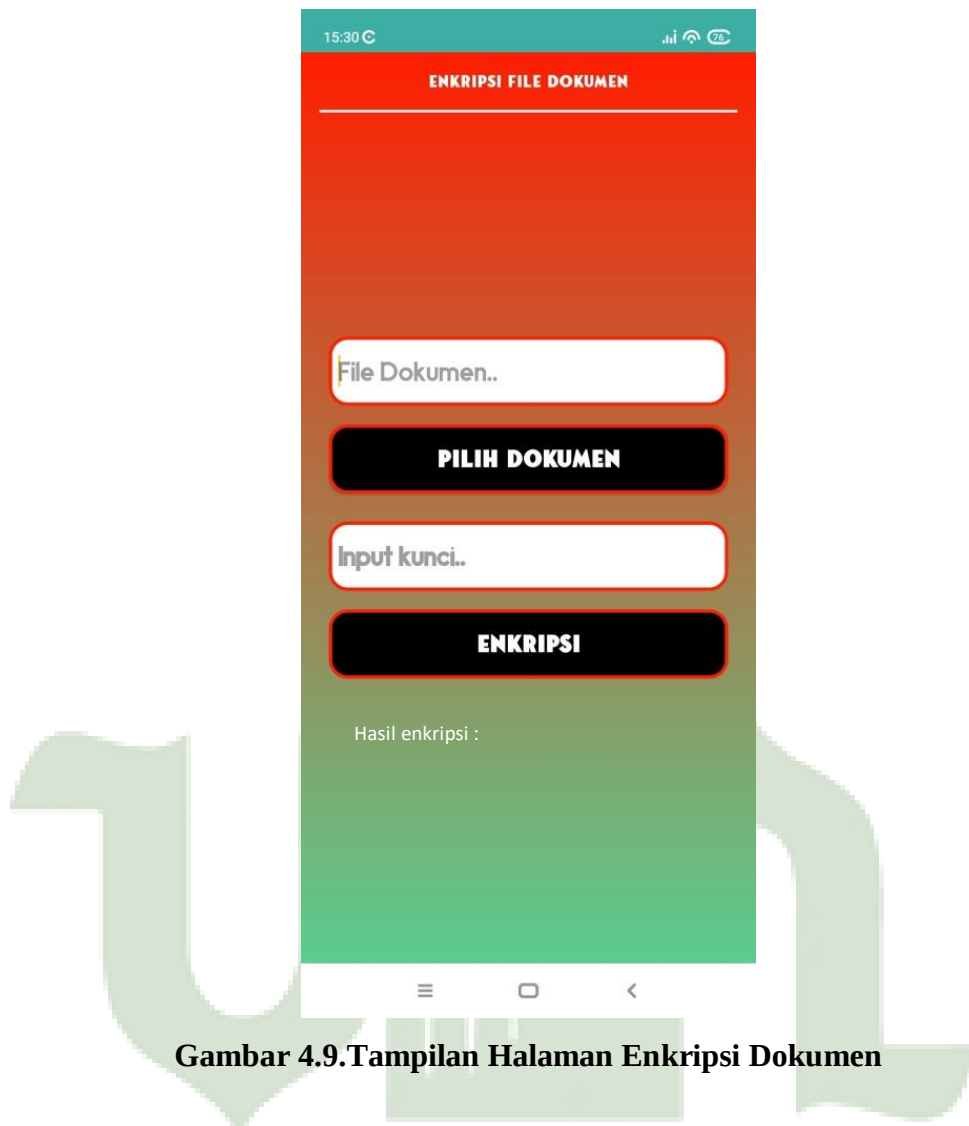
Proses enkripsi dokumen merupakan fitur penting dalam sistem keamanan digital yang memungkinkan pengguna melindungi informasi sensitif. Sistem ini dirancang khusus untuk mengenkripsi dokumen dengan mendukung tiga jenis file utama: Microsoft Word, Microsoft Excel, dan PDF. Ketika pengguna ingin mengamankan dokumennya, mereka harus memulai proses dengan mengakses halaman enkripsi dan mengklik ikon enkripsi yang tersedia.

Tahapan enkripsi dimulai dengan memilih file yang ingin diamankan dari penyimpanan komputer. Sistem memiliki batasan ketat bahwa hanya file berekstensi .docx, .doc, .xlsx, .xls, dan .pdf yang dapat diproses. Setelah memilih file, pengguna wajib memasukkan kunci enkripsi yang terdiri dari empat karakter huruf. Kunci ini berperan kunci dalam mengamankan dokumen dan nantinya akan digunakan untuk membuka kembali file yang telah dienkripsi.

Proses enkripsi berlangsung secara otomatis setelah pengguna menekan tombol enkripsi. Sistem akan langsung memverifikasi file, mengubah konten dokumen menjadi format terenkripsi, dan menghasilkan file baru yang terlindungi. Penting bagi pengguna untuk memahami bahwa kehilangan kunci enkripsi berarti dokumen tidak dapat dibuka kembali, sehingga penyimpanan kunci dengan aman menjadi hal kritis dalam proses ini.

Keunggulan utama sistem enkripsi ini terletak pada kesederhanaan penggunaan dan tingkat keamanan yang tinggi. Dengan hanya menggunakan empat karakter huruf, pengguna dapat melindungi dokumen penting dari akses tidak sah. Sistem memberikan lapisan keamanan tambahan bagi individu dan organisasi yang memerlukan perlindungan dokumen digital, memungkinkan mereka mengontrol dan membatasi akses informasi sensitif. Tampilan halaman enkripsi dokumen dapat dilihat pada gambar 4.9.

SUMATERA UTARA MEDAN



Gambar 4.9. Tampilan Halaman Enkripsi Dokumen

2. Tampilan Halaman Dekripsi Dokumen

Dekripsi dokumen merupakan tahap krusial dalam manajemen keamanan file digital, yang memungkinkan pengguna untuk mengembalikan dokumen terenkripsi menjadi format aslinya yang dapat dibaca. Setelah proses enkripsi dilakukan, pengguna memerlukan prosedur khusus untuk membuka kembali dokumen yang telah diamankan. Menu dekripsi dokumen dirancang secara spesifik untuk memfasilitasi proses pembukaan file yang sebelumnya telah dienkripsi, memberikan kontrol penuh kepada pemilik dokumen untuk mengakses kembali informasi pentingnya.

Proses dekripsi dimulai dengan mengakses halaman khusus dekripsi dokumen dan mengidentifikasi file terenkripsi yang ingin dibuka. Pengguna harus melakukan beberapa langkah kunci, diawali dengan menekan ikon dekripsi yang tersedia di antarmuka sistem. Selanjutnya, pengguna akan diminta untuk memilih file terenkripsi dari penyimpanan yang tersedia. Tahap kritis dalam proses ini adalah memasukkan kunci dekripsi, yang harus sama persis dengan kunci enkripsi yang digunakan sebelumnya - terdiri dari empat karakter huruf.

Sistem dekripsi dirancang dengan mekanisme keamanan tinggi yang memastikan hanya pemilik dokumen yang sah yang dapat membuka file. Setelah memilih file dan memasukkan kunci yang benar, pengguna cukup menekan ikon dekripsi, dan sistem akan secara otomatis memproses pembukaan dokumen. Proses ini berlangsung cepat dan instan, mengembalikan file ke format aslinya - baik itu dokumen Word, Excel, atau PDF - sehingga pengguna dapat segera mengakses dan menggunakan kembali dokumen tersebut.

Fitur tambahan yang penting dalam proses dekripsi adalah keberadaan ikon hasil dekripsi di bagian bawah halaman. Fitur ini memungkinkan pengguna untuk dengan mudah mengidentifikasi lokasi penyimpanan file yang telah berhasil didekripsi. Hal ini sangat membantu dalam manajemen file, memastikan pengguna dapat dengan cepat menemukan dan menggunakan kembali dokumen yang baru saja dibuka. Keamanan menjadi fokus utama dalam desain sistem dekripsi ini. Proses dekripsi dirancang sedemikian rupa sehingga hanya mereka yang mengetahui kunci enkripsi yang dapat membuka dokumen. Konsekuensi dari kehilangan atau salah memasukkan kunci adalah dokumen tetap terenkripsi dan tidak dapat dibuka, yang memberikan lapisan perlindungan tambahan terhadap potensi akses tidak sah. Dengan demikian, sistem dekripsi tidak hanya sekadar alat pembuka file, melainkan juga mekanisme keamanan yang canggih untuk melindungi informasi sensitif.

Pentingnya kehati-hatian dalam proses dekripsi tidak dapat dikesampingkan. Pengguna harus selalu memastikan menyimpan kunci enkripsi dengan aman, mencatat kombinasi huruf yang digunakan, dan menghindari berbagi kunci dengan pihak yang tidak berwenang. Setiap kesalahan dalam memasukkan kunci dapat berarti kehilangan akses permanen ke dokumen, yang dapat berdampak signifikan terutama untuk file-file penting yang mengandung informasi kritis. Tampilan halaman dekripsi file dokumen dapat dilihat pada gambar 4.10.



Gambar 4.10. Tampilan Halaman Dekripsi Dokumen

3. Tampilan Halaman Tentang Aplikasi

Halaman tentang aplikasi menampilkan informasi dari pelaksana penelitian. Pada halaman tentang aplikasi terdapat logo, yang mana logo yang akan digunakan adalah logo Universitas Islam Negeri Sumatera Utara. Kemudian biodata dari peneliti berupa nama peneliti, yaitu Muhaimi Rizki Siregar dan nim peneliti, yaitu 0701173195. Pada halaman tentang aplikasi juga dicantumkan judul penelitian yang dilaksanakan oleh peneliti dalam menghasilkan aplikasi keamanan file dokumen. Tampilan halaman tentang aplikasi pada aplikasi dapat dilihat pada gambar 4.11.



Gambar 4.11. Tampilan Halaman Tentang Aplikasi

4.2.3 Hasil Pengujian Aplikasi

Dalam pengujian penelitian akan melakukan proses enkripsi dan dekripsi beberapa dokumen word, dokumen excel dan dokumen PDF. Pada gambar dapat dilihat bahwa ukuran file sebelum dienkripsi adalah 12,49 KB dengan kunci okey, dimana hanya terdapat empat karakter huruf. Setelah proses deskripsi file dokumen tersebut berubah ukuran menjadi 12,5 KB dengan kunci yang sama dengan proses enkripsi sebelumnya. Jadi, dapat disimpulkan bahwa file sebelum dienkripsi dan sesudah dideskripsi dapat berubah ukurannya dan bisa jugak tidak. Harus diperhatikan adalah saat menginputkan kunci kedua proses tersebut. Hasil pengujian dapat dilihat pada tabel 4.3.

Tabel 4.3. Hasil Pengujian Aplikasi

No	Enkripsi	Dekripsi	Keterangan
1			Ukuran awal file : 12,49 KB Plaintext : dokumenword.docx Kunci : okey Ciphertext : 7an,9cwKvPD oCeC5.mhi Ukuran akhir file : 12,5 KB

2	 	Ukuran awal file : 8,71 KB Plaintext : pengamananexcel.xlsx Kunci : siap Ciphertext : SpZlReTPy45l2s9urSUD.m hi Ukuran akhir file : 8,71 KB
3	 	Ukuran awal file : 178,13 KB Plaintext : pdfrahasia.pdf Kunci : test Ciphertext : Q4xcLfrCTerLle.mhi Ukuran akhir file : 178,14 KB