BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, keamanan data menjadi aspek yang sangat penting dalam pengembangan sistem informasi, termasuk dalam sektor bisnis kuliner seperti coffee shop. Kemajuan teknologi telah mendorong pelaku usaha untuk beralih ke sistem digital guna mendukung operasional sehari-hari, salah satunya dalam proses pemesanan, reservasi, dan transaksi. Namun, banyak sistem yang dibangun masih mengabaikan perlindungan data, terutama data transaksi yang bersifat sensitif.

Coffee Shop Mene Ngopi yang berdiri sejak tahun 2020 saat ini masih menerapkan proses pemesanan dan reservasi secara langsung di tempat. Pelanggan harus datang ke lokasi, mengantre di kasir, memesan makanan dan minuman, serta menunggu ketersediaan tempat duduk tanpa sistem reservasi yang terintegrasi. Selain menyebabkan kepadatan saat jam sibuk, metode ini juga menyimpan potensi risiko terhadap manipulasi atau kehilangan data transaksi. Informasi penting seperti nominal pembayaran, waktu transaksi, dan identitas pelanggan tidak dicatat dan disimpan dengan perlindungan digital yang layak (Jusin dkk., 2020).

Selain itu, pengelolaan tempat duduk di Mene Ngopi belum mendukung pengaturan ruang yang sesuai dengan kondisi jumlah pengunjung. Meja-meja besar sering kali hanya ditempati satu atau dua orang, sementara pengunjung lain tidak mendapatkan tempat duduk karena terlihat seolah semua meja sudah terisi. Hal ini menyebabkan penggunaan ruang menjadi tidak maksimal dan menciptakan kesan penuh, meskipun sebenarnya masih terdapat kapasitas yang tersedia.

Dalam konteks ini, penerapan sistem digital yang tidak hanya mendukung proses pemesanan dan reservasi, tetapi juga mampu menjaga kerahasiaan dan integritas data menjadi hal yang sangat dibutuhkan. Algoritma kriptografi seperti Advanced Encryption Standard (AES) dapat digunakan untuk

mengenkripsi data transaksi agar tidak mudah diakses atau diubah oleh pihak yang tidak berwenang. AES merupakan algoritma enkripsi simetris yang terbukti aman dan digunakan secara luas untuk melindungi informasi penting di berbagai sektor (Putra dkk., 2023).

Dengan menerapkan enkripsi AES, data transaksi dalam sistem pemesanan dan reservasi dapat disimpan dalam bentuk terenkripsi (ciphertext), sehingga hanya pihak yang memiliki kunci yang dapat membaca isinya. Pendekatan ini tidak hanya meningkatkan keamanan data, tetapi juga memberikan kepercayaan lebih kepada pelanggan terhadap sistem digital yang digunakan.

Kriptografi merupakan disiplin ilmu yang bertujuan untuk melindungi keamanan informasi melalui berbagai teknik yang digunakan untuk mengamankan pesan atau data, sehingga hanya pihak yang memiliki hak akses yang dapat mengaksesnya. Proses utama dalam kriptografi mencakup dua komponen penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses yang mengubah pesan atau data dengan menggunakan algoritma tertentu, dan hanya dapat dikembalikan ke bentuk aslinya oleh pihak yang memiliki kunci enkripsi yang sesuai. Kunci ini dapat bersifat simetris atau asimetris. Sementara itu, dekripsi adalah proses yang mengembalikan informasi atau pesan yang telah dienkripsi ke bentuk semula. Pada tahap ini, pesan atau data diolah menggunakan algoritma kriptografi dan kunci enkripsi untuk menjaga kerahasiaannya (Pramono dkk., 2024).

Data yang bersifat sensitif, seperti data transaksi, memerlukan perlindungan khusus. Data transaksi mencakup informasi pembayaran yang bersifat rahasia dan perlu dijaga agar tidak disalahgunakan. Oleh karena itu, diperlukan algoritma yang mampu mengenkripsi data sensitif ini, sehingga pihak yang tidak memiliki hak akses tidak dapat mengetahui isi dari data tersebut (M. R. Andriyanto & Sukmasetya, 2022).

Berdasarkan uraian diatas yang telah disampaikan, maka penulis tertarik untuk mengambil judul "**Rancang Bangun Aplikasi Pemesanan Menggunakan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Di Coffee Shop Mene Ngopi**".

1.2 Identifikasi Masalah

Berdasarkan uraian latar belakang diatas, maka permasalahan yang terjadi dapat didentifikasi sebagai berikut :

1. Proses pemesanan dan reservasi di Coffee Shop Mene Ngopi masih dilakukan secara manual, yang menyebabkan antrean panjang dan meningkatkan potensi kesalahan dalam pencatatan pesanan.
2. Pengaturan tempat duduk belum mendukung pengelolaan ruang yang sesuai dengan kondisi pengunjung, sehingga menciptakan kesan penuh meskipun masih tersedia kapasitas.
3. Data transaksi pelanggan tidak diamankan dengan sistem digital yang memadai, sehingga berisiko mengalami manipulasi, pencurian, atau kehilangan informasi penting.

1.3 Rumusan Masalah

Berdasarkan pada latar belakang dan pembahasan yang dipaparkan diatas, maka rumusan masalah dalam peneliti ini adalah sebagai berikut :

1. Bagaimana merancang dan membangun aplikasi pemesanan dan reservasi yang dapat membantu pelanggan melakukan pemesanan tanpa harus mengantre dan meminimalkan kesalahan dalam pencatatan pesanan?
2. Bagaimana merancang sistem pengelolaan tempat duduk yang dapat mendukung pemanfaatan ruang agar lebih teratur dan sesuai dengan jumlah pengunjung?
3. Bagaimana penerapan algoritma Advanced Encryption Standard (AES) dalam aplikasi pemesanan dan reservasi untuk menjaga kerahasiaan dan keutuhan data transaksi dari akses atau perubahan yang tidak sah?

1.4 Batasan Masalah

Agar pembahasan masalah menjadi lebih jelas dan terarah maka diperlukan adanya batasan masalah. Adapun ruang lingkup permasalahan dibatasi oleh:

1. Penelitian ini dilakukan di Coffee Shop Mene Ngopi dan difokuskan pada proses pemesanan, reservasi tempat duduk, dan pengamanan data transaksi pelanggan.

2. Kode transaksi dalam aplikasi ini dirancang untuk memberikan identifikasi unik pada setiap transaksi. Format kode transaksi terdiri dari beberapa elemen yang digabungkan menjadi satu string, sehingga mudah dikenali dan dikelola oleh sistem. Berikut struktur kode transaksi yang digunakan:

   [PREFIX][TANGGAL][NOMOR URUT]

   Keterangan :

   a. [PREFIX]: Awalan untuk membedakan jenis transaksi.
   b. [TANGGAL]: Tanggal transaksi dalam format YYYYMMDD (tahun, bulan, dan hari), untuk menunjukkan kapan transaksi terjadi.
   c. [NOMOR URUT]: Nomor urut transaksi pada hari tersebut untuk menjaga keunikan setiap transaksi.

   Contoh Kode Transaksi: MENE202410090001
3. Aplikasi ini memiliki empat jenis hak akses:
   a. Pimpinan: Memiliki akses penuh untuk memeriksa laporan data transaksi.
   b. Kasir: Bertanggung jawab mengelola pembayaran, memproses pesanan, dan mengubah status transaksi. Untuk menampilkan data pesanan, kasir dapat memindai QR code yang diberikan pelanggan. Setelah dipindai, sistem akan mendekripsi kode transaksi dan menampilkan detail pesanan jika kode transaksi cocok.
   c. Pelanggan: Dapat melihat menu, pemesanan, memeriksa status pesanan, dan menyelesaikan pembayaran. Untuk keamanan, data transaksi akan dienkripsi sebelum disimpan. Kode transaksi dienkripsi menggunakan algoritma AES, lalu disimpan di basis data. Sistem kemudian menghasilkan QR code dari kode enkripsi untuk mempermudah menampilkan data transaksi.
   d. Koki: Mengelola pesanan yang masuk dan memperbarui status pesanan saat selesai diproses atau ditolak karena stok tidak tersedia.
4. Sistem ini akan dibangun menggunakan bahasa pemrograman HTML, CSS, JavaScript, dan PHP serta database MySQL.

5. Aplikasi ini menggunakan algoritma AES 128-bit untuk mengenkripsi kode transaksi yang disimpan, memastikan bahwa keamanan data tetap terjaga meskipun ada upaya peretasan.

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini yaitu :

1. Membangun aplikasi pemesanan dan reservasi yang dapat memfasilitasi pelanggan dalam melakukan pemesanan secara langsung melalui sistem digital, sekaligus mengurangi kepadatan antrian dan potensi kesalahan pencatatan.
2. Menyediakan fitur pengaturan tempat duduk yang dapat membantu pengelola dalam menyusun alokasi meja agar sesuai dengan kondisi pengunjung yang datang.
3. Menerapkan algoritma Advanced Encryption Standard (AES) untuk mengamankan data transaksi, sehingga informasi bersifat rahasia tidak dapat diakses atau dimanipulasi oleh pihak yang tidak berwenang.

1.6 Manfaat Penelitian

Adapun manfaat penelitian antara lain :

1.6.1 Manfaat Teoretis

Hasil dari penelitian ini adalah untuk meningkatkan pemahaman dalam merancang dan mengembangkan aplikasi berbasis web, serta memperdalam pengetahuan mengenai implementasi algoritma kriptografi, khususnya AES, dalam konteks keamanan data transaksi. Selain itu, penelitian ini juga dapat memperkaya wawasan tentang penerapan teknologi dalam menyelesaikan masalah bisnis yang nyata. Dengan demikian, hasil dari penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan teori di bidang keamanan data, pengembangan aplikasi web, dan penerapan teknologi dalam dunia bisnis.

1.6.2 Manfaat Praktis

Hasil penelitian yang dilakukan oleh peneliti diharapkan pula dapat memberikan kegunaan atau manfaat praktis bagi beberapa pihak yaitu:

1. Bagi Coffee Shop
    a. Menyediakan sistem pemesanan dan reservasi yang mempermudah proses transaksi dan pelayanan kepada pelanggan.
    b. Membantu pengelola dalam menyusun tempat duduk sesuai kebutuhan harian pengunjung.
    c. Menjaga keamanan informasi transaksi dari gangguan atau penyalahgunaan, sehingga dapat menghindari risiko kehilangan atau manipulasi data.
2. Bagi Pelanggan
    a. Memberikan kenyamanan dalam melakukan pemesanan dan reservasi tanpa perlu hadir secara langsung ke lokasi terlebih dahulu.
    b. Menjamin bahwa informasi pembayaran dan data pribadi yang disampaikan tetap terlindungi.
    c. Meningkatkan rasa aman dan kepercayaan dalam menggunakan layanan digital Mene Ngopi.

1.7 Pertanyaan Penelitian

Dari masalah yang telah diidentifikasi sebelumnya, maka terdapat beberapa pertanyaan sebagai berikut:

1. Apakah aplikasi pemesanan dan reservasi yang dibangun dapat membantu mengurangi kepadatan antrean dan meminimalkan kesalahan dalam pencatatan pesanan?
2. Apakah sistem pengelolaan tempat duduk dapat membantu pengaturan ruang yang sesuai dengan kondisi pengunjung?
3. Apakah penerapan algoritma AES mampu menjaga keamanan data transaksi dari akses atau perubahan yang tidak sah?

1.8 Hipotesis Penelitian

Dengan adanya penelitian berjudul "Rancang Bangun Aplikasi Pemesanan Menggunakan Algoritma Advanced Encryption Standard (AES) Untuk

Keamanan Data Transaksi di Coffee Shop Mene Ngopi," diharapkan aplikasi dan algoritma yang dikembangkan dapat memberikan hasil sebagai berikut:

1. Aplikasi pemesanan dan reservasi digital yang dilengkapi fitur pengelolaan tempat duduk dapat membantu mengurangi antrian dan kesalahan pencatatan.
2. Penerapan algoritma AES dalam sistem pemesanan dan reservasi dapat menjaga kerahasiaan dan keutuhan data transaksi pelanggan dari potensi ancaman pihak tidak berwenang.

1.9 Metodologi Penelitian

Metode penelitian merupakan tahapan-tahapan yang dilakukan oleh peneliti untuk menyelesaikan permasalahan yang hendak diselesaikan. Peneliti menggunakan beberapa metode untuk menyelesaikan penelitian ini, yaitu :

1.9.1 Metode Pengumpulan Data

1. Studi Pustaka

   Studi kepustakaan atau studi pustaka adalah kajian teoritis yang mencakup referensi serta literatur ilmiah lainnya yang berkaitan dengan budaya, nilai, dan norma dalam konteks sosial yang diteliti (Cahyono, 2020). Penelitian ini menggunakan sumber-sumber seperti jurnal, buku, dan internet untuk mengumpulkan informasi. Peneliti menganalisis literatur yang relevan untuk memahami konsep-konsep dan teori yang mendukung penggunaan algoritma AES dan aplikasi berbasis website. Dari analisis ini, peneliti menyusun dasar teori yang menjadi acuan dalam penelitian dan merumuskan hipotesis yang akan diuji. Studi pustaka ini menjadi landasan untuk menggali informasi yang berkaitan dengan topik yang diteliti.

2. Observasi

   Observasi adalah proses pengamatan sistematis terhadap aktivitas manusia dan pengaturan fisik di mana kegiatan tersebut berlangsung secara terus-menerus dari lokus aktivitas yang bersifat alami untuk menghasilkan fakta (Pratiwi dkk., 2023). Penelitian ini

dilakukan dengan mengamati langsung Coffee Shop Mene Ngopi untuk mengidentifikasi masalah dalam pemesanan dan pengelolaan tempat duduk. Peneliti mengamati bagaimana proses pemesanan dilakukan oleh pelanggan dan staf, serta bagaimana tempat duduk diatur untuk mengakomodasi pengunjung. Peneliti juga mencatat masalah yang muncul dalam kedua aspek tersebut untuk mendapatkan gambaran tentang tantangan yang dihadapi dan cara-cara untuk meningkatkan sistem yang ada.

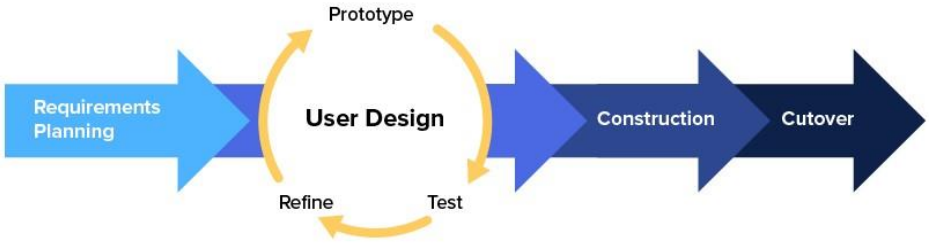
3. Wawancara

   Wawancara adalah kegiatan yang mempertemukan dua individu untuk melakukan pertukaran informasi dan ide melalui tanya jawab, sehingga dihasilkan kesimpulan terkait topik tertentu (Irawan dkk., 2024). Penelitian ini dilakukan melalui wawancara langsung dengan Mas Galih Fikriansyah, pemilik Coffee Shop Mene Ngopi, untuk mengidentifikasi masalah yang ada di kedai. Dalam wawancara tersebut, peneliti menggali informasi mengenai proses pemesanan dan pengelolaan tempat duduk, serta solusi yang akan diberikan untuk meningkatkan layanan dan pengelolaan kedai.

1.9.2 Metode Pengembangan Sistem

Dalam penelitian ini, pengembangan aplikasi untuk pemesanan dilakukan menggunakan pendekatan RAD (Rapid Application Development). RAD (Rapid Application Development) merupakan salah satu metode pengembangan sistem informasi yang memungkinkan penyelesaian dalam waktu yang relatif singkat dan efisien (Bilah dkk., 2022). Metode RAD memiliki keunggulan dalam memberikan hasil lebih cepat dan meningkatkan fleksibilitas selama proses pengembangan. Keunggulan utama RAD adalah kemampuannya mempercepat waktu pengembangan, yang sangat berguna dalam lingkungan bisnis yang cepat berubah dan kompetitif. Metode ini memungkinkan pengembang untuk dengan cepat membuat

prototipe perangkat lunak, sehingga umpan balik dari pengguna dapat segera diperoleh dan diintegrasikan dalam pengembangan. Hal ini memungkinkan RAD untuk dengan cepat menyesuaikan diri dengan perubahan kebutuhan atau persyaratan, sehingga mengurangi risiko kegagalan proyek (Aristo dkk., 2024).



Gambar 1. 1 Tahapan Metodologi RAD (Aristo dkk., 2024)

Untuk proses yang dilakukan pada penelitian ini secara terinci setiap tahap yang ada pada Gambar 1.1, dijelaskan sebagai berikut:

1. Requirements Planning (Perencanaan Persyaratan)

   Pada tahap ini, masalah utama di Coffee Shop Mene Ngopi akan diidentifikasi dengan menggunakan metode studi pustaka, observasi, dan wawancara. Studi pustaka akan mengumpulkan dan menganalisis informasi dari sumber-sumber yang berkaitan. Observasi akan melihat kondisi operasional sehari-hari, seperti interaksi pelanggan, layanan, dan pengelolaan tempat duduk. Wawancara dengan pemilik akan memberikan informasi langsung tentang masalah yang dihadapi. Gabungan ketiga metode ini akan membantu menemukan masalah utama dan merumuskan solusi yang tepat.
2. User Design (Desain Pengguna)

   Pada tahap ini, perancangan sistem fokus pada cara pengguna (seperti pimpinan, kasir, pelanggan, dan koki) berinteraksi dengan sistem. Interaksi ini digambarkan menggunakan diagram UML yang dibuat dengan StarUML dan

Draw.io. Diagram Use Case menunjukkan cara setiap peran menggunakan sistem, sementara diagram lain seperti Activity Diagram, Sequence Diagram, dan Class Diagram menggambarkan alur kerja, interaksi antar-komponen, dan struktur sistem. Selain itu, Rich Picture Diagram juga dibuat untuk memberikan gambaran visual tentang keseluruhan sistem, termasuk hubungan antar aktor dan proses seperti pemesanan, pembayaran, dan pengelolaan pesanan.

3. Construction (Konstruksi)

   Pada tahap ini, pengembangan sistem dilakukan berdasarkan desain yang telah dibuat sebelumnya. Aplikasi dibangun menggunakan beberapa teknologi, yaitu HTML dan CSS untuk membuat antarmuka pengguna yang responsif, JavaScript untuk interaksi dinamis pada halaman web, serta PHP sebagai bahasa pemrograman server-side yang mengelola logika bisnis dan interaksi dengan database.

4. Cutover (Pemindahan)

   Tahap ini merupakan proses akhir di mana aplikasi yang telah dikembangkan dipindahkan dari lingkungan pengembangan ke lingkungan produksi. Pada tahap ini, dilakukan pengujian akhir, termasuk Black Box Testing untuk memeriksa fungsionalitas sistem dari sisi antarmuka dan hasil keluaran tanpa melihat kode, serta White Box Testing untuk memastikan logika internal dan alur program berjalan dengan benar. Selain itu, dilakukan User Acceptance Testing (UAT) di mana pengguna akhir (pimpinan, kasir, pelanggan, dan koki) akan menguji aplikasi untuk memastikan bahwa semua fitur bekerja sesuai dengan kebutuhan dan harapan.

1.9.3 Metode Penyelesaian Masalah

AES (Advanced Encryption Standard) merupakan metode

kriptografi simetris untuk melindungi informasi. Ini menjadi standar dalam enkripsi menggunakan kunci yang sama untuk enkripsi dan dekripsi (Ahmad Sitorus dkk., 2020). Dalam algoritma AES, tabel ASCII menjadi salah satu komponen penting, karena tabel ini digunakan untuk merepresentasikan karakter alfanumerik dalam bentuk kode yang dapat diproses oleh komputer. Pengubahan karakter ke dalam bentuk kode ASCII merupakan langkah awal yang penting sebelum data masuk ke proses enkripsi yang lebih kompleks dalam algoritma AES.

Tabel ASCII sendiri merupakan kumpulan kode alfanumerik yang digunakan untuk mewakili angka, huruf, simbol, dan karakter khusus di dalam komputer. ASCII, yang merupakan singkatan dari American Standard Code for Information Interchange, terdiri dari 128 karakter yang direpresentasikan menggunakan 7 bit (berkisar dari 00 hingga 7F dalam format heksadesimal). Dari 128 karakter tersebut, 32 karakter pertama merupakan perintah non-grafis, seperti "null", "escape", dan lainnya, yang berfungsi sebagai urutan kontrol. Sementara itu, karakter lainnya merupakan simbol grafis yang dapat ditampilkan, seperti huruf, angka, dan berbagai simbol lainnya. Tabel berikut menunjukkan seluruh karakter ASCII beserta kodenya (VLSIFacts, 2023).

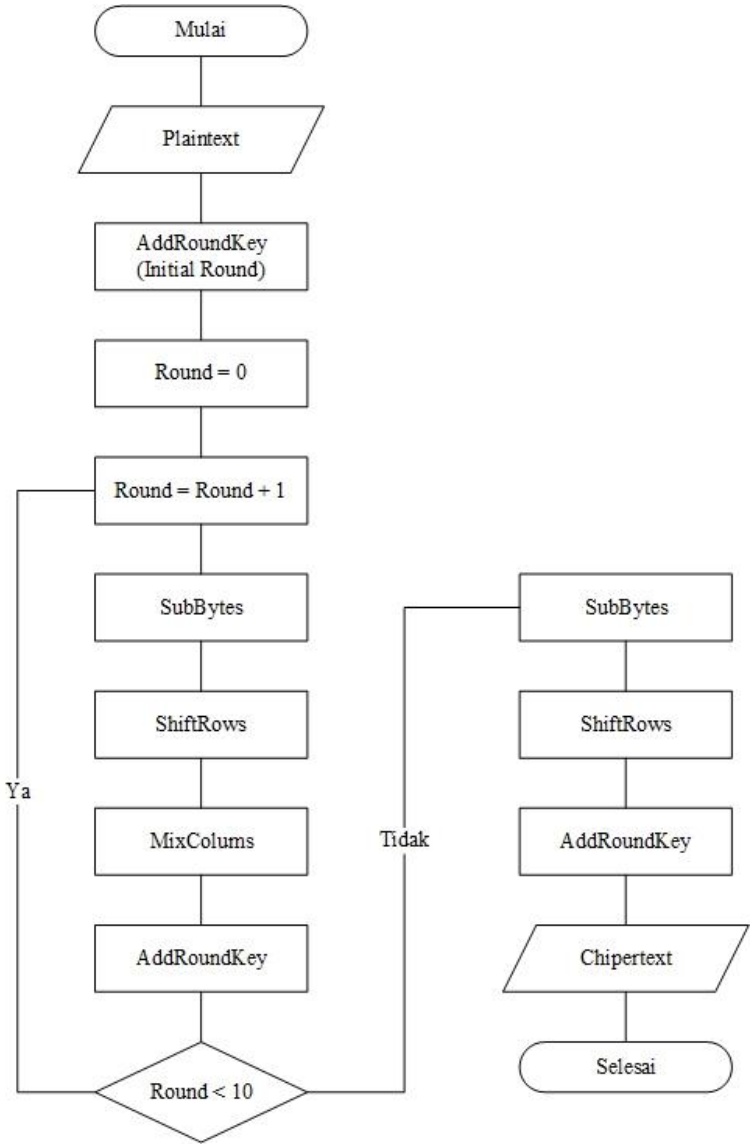
Control Characters				Graphic Symbols											
Name	Dec	Binary	Hex	Symbol	Dec	Binary	Hex	Symbol	Dec	Binary	Hex	Symbol	Dec	Binary	Hex
NUL	0	0000000	00	space	32	0100000	20	@	64	1000000	40	`	96	1100000	60
SOH	1	0000001	01	!	33	0100001	21	A	65	1000001	41	a	97	1100001	61
STX	2	0000010	02	"	34	0100010	22	B	66	1000010	42	b	98	1100010	62
ETX	3	0000011	03	#	35	0100011	23	C	67	1000011	43	c	99	1100011	63
EOT	4	0000100	04	$	36	0100100	24	D	68	1000100	44	d	100	1100100	64
ENQ	5	0000101	05	%	37	0100101	25	E	69	1000101	45	e	101	1100101	65
ACK	6	0000110	06	&	38	0100110	26	F	70	1000110	46	f	102	1100110	66
BEL	7	0000111	07	'	39	0100111	27	G	71	1000111	47	g	103	1100111	67
BS	8	0001000	08	(	40	0101000	28	H	72	1001000	48	h	104	1101000	68
HT	9	0001001	09	)	41	0101001	29	I	73	1001001	49	i	105	1101001	69
LF	10	0001010	0A	*	42	0101010	2A	J	74	1001010	4A	j	106	1101010	6A
VT	11	0001011	0B	+	43	0101011	2B	K	75	1001011	4B	k	107	1101011	6B
FF	12	0001100	0C	,	44	0101100	2C	L	76	1001100	4C	l	108	1101100	6C
CR	13	0001101	0D	−	45	0101101	2D	M	77	1001101	4D	m	109	1101101	6D
SO	14	0001110	0E	.	46	0101110	2E	N	78	1001110	4E	n	110	1101110	6E
SI	15	0001111	0F	/	47	0101111	2F	O	79	1001111	4F	o	111	1101111	6F
DLE	16	0010000	10	0	48	0110000	30	P	80	1010000	50	p	112	1110000	70
DC1	17	0010001	11	1	49	0110001	31	Q	81	1010001	51	q	113	1110001	71
DC2	18	0010010	12	2	50	0110010	32	R	82	1010010	52	r	114	1110010	72
DC3	19	0010011	13	3	51	0110011	33	S	83	1010011	53	s	115	1110011	73
DC4	20	0010100	14	4	52	0110100	34	T	84	1010100	54	t	116	1110100	74
NAK	21	0010101	15	5	53	0110101	35	U	85	1010101	55	u	117	1110101	75
SYN	22	0010110	16	6	54	0110110	36	V	86	1010110	56	v	118	1110110	76
ETB	23	0010111	17	7	55	0110111	37	W	87	1010111	57	w	119	1110111	77
CAN	24	0011000	18	8	56	0111000	38	X	88	1011000	58	x	120	1111000	78
EM	25	0011001	19	9	57	0111001	39	Y	89	1011001	59	y	121	1111001	79
SUB	26	0011010	1A	:	58	0111010	3A	Z	90	1011010	5A	z	122	1111010	7A
ESC	27	0011011	1B	;	59	0111011	3B	[	91	1011011	5B	{	123	1111011	7B
FS	28	0011100	1C	<	60	0111100	3C	\	92	1011100	5C	|	124	1111100	7C
GS	29	0011101	1D	=	61	0111101	3D	]	93	1011101	5D	}	125	1111101	7D
RS	30	0011110	1E	>	62	0111110	3E	^	94	1011110	5E	~	126	1111110	7E
US	31	0011111	1F	?	63	0111111	3F	_	95	1011111	5F	Del	127	1111111	7F

Gambar 1. 2 Tabel ASCII Code (VLSIFacts, 2023).

1. Proses Ekspansi Kunci

   Proses ekspansi kunci pada Algoritma Advanced Encryption Standard (AES) dimulai dengan mengambil kunci cipher, yang kemudian diperluas melalui proses ekspansi kunci untuk membentuk key schedule (Ahmad Sitorus dkk., 2020).

2. Proses Enkripsi



Gambar 1. 3 Flowchart Enkripsi AES – 128

Enkripsi merupakan sebuah teknik yang dilakukan mengacak data asli menjadi kode rahasia sehingga menyulitkan orang yang tidak berkepentingan untuk mengakses dan mengetahui data yang asli (Setyawan dkk., 2024). Proses enkripsi dalam algoritma AES-128 melibatkan empat jenis transformasi byte, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Di awal proses, state mengalami transformasi byte melalui AddRoundKey. Selanjutnya, state

akan melalui serangkaian transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang sebanyak Nr (jumlah ronde). Proses berulang ini dikenal sebagai round function. Namun, pada ronde terakhir, ada perbedaan di mana state tidak lagi melalui transformasi MixColumns (R. Andriyanto dkk., 2020).

Secara garis besar proses enkripsi AES-128 dengan kunci 128 bit adalah sebagai berikut:

a. AddRoundKey: melakukan XOR antara state awal (plainteks) dengan cipher key. Pada Tahap ini disebut juga initial round.
b. Round : Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
    1. SubBytes: substitusi byte dengan menggunakan tabel substitusi (Sbox).

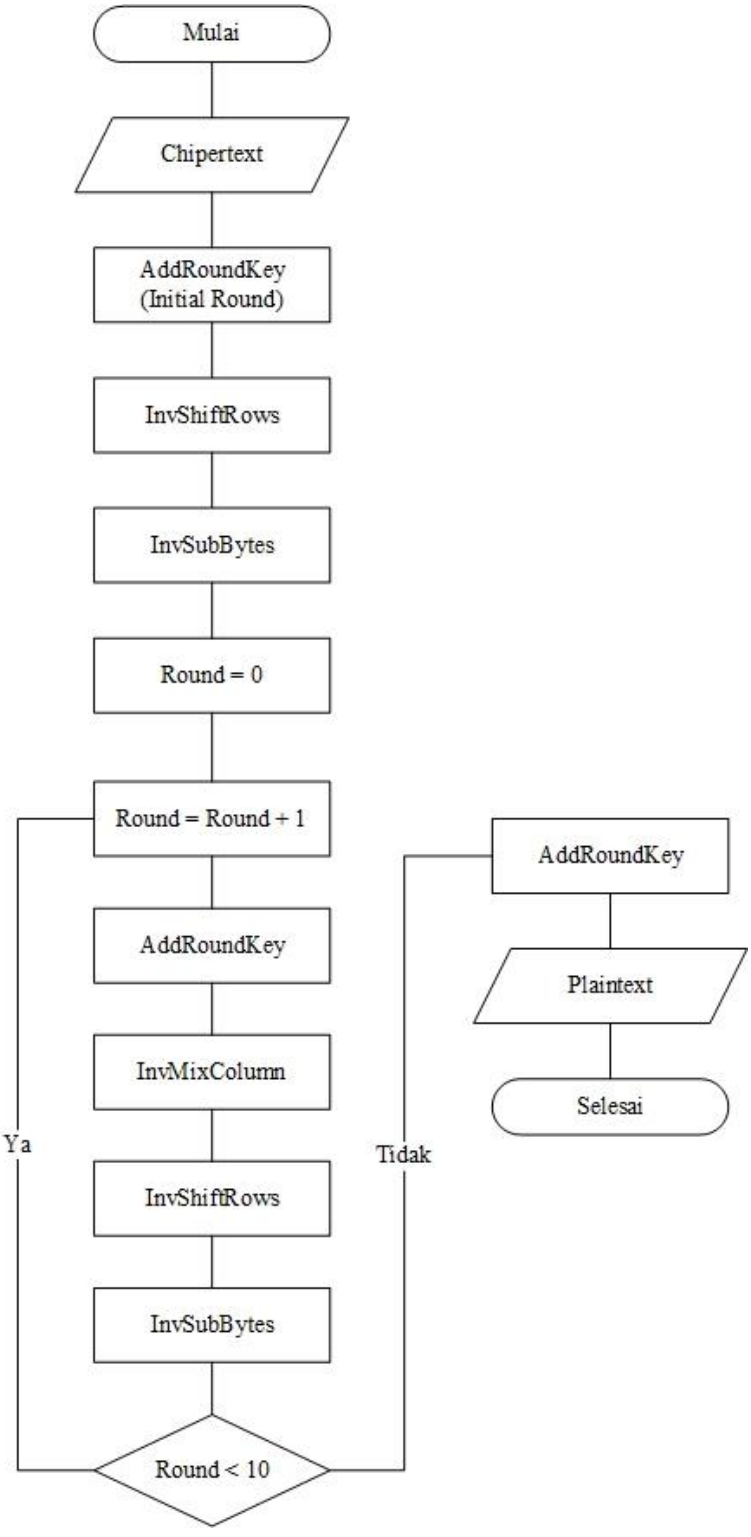
	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 1. 4 Table S-Box (R. Andriyanto dkk., 2020)

    2. ShiftRows: pergeseran baris-baris array state secara wrapping.
c. MixColumns: mengacak data pada masing-masing kolom array state dengan persamaan sebagai berikut:
   $A(x) = \{03\}x2 \oplus \{01\}x2 \oplus \{01\}x2 \oplus \{02\}(1)$

d. AddRoundKey: melakukan XOR antara state sekarang round key.
e. Final Round: proses untuk putaran terakhir antara lain:
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey
f. Pada proses terakhir akan menghasilkan karakter atau teks yang berbentuk chipertext.

3. Proses Dekripsi



Gambar 1. 5 Flowchart Dekripsi AES – 128

Dekripsi merupakan proses yang berlawanan dengan

enkripsi, di mana fungsinya adalah untuk mengembalikan data yang telah terenkripsi menjadi bentuk aslinya. Dengan dekripsi, data yang sebelumnya diubah menjadi kode rahasia dikonversi kembali menjadi data yang dapat dibaca seperti semula (Setyawan dkk., 2024). Proses dekripsi pada AES-128 memerlukan pembalikan transformasi cipher untuk menghasilkan inverse cipher, yang melibatkan beberapa tahap, yaitu: InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey (R. Andriyanto dkk., 2020).

Secara garis besar proses dekripsi AES-128 dengan kunci 128 bit adalah sebagai berikut :

a. AddRoundKey (Initial Round): XOR dilakukan antara ciphertext dan round key untuk memulai proses dekripsi.
b. InvShiftRows:: Setiap baris pada state dipindahkan ke kanan untuk memulihkan posisi awal byte.
c. InvSubBytes: Setiap elemen pada state diubah menggunakan tabel S-Box untuk mengembalikan nilai byte yang asli.
d. Round: Proses dekripsi dilanjutkan dengan melakukan langkah-langkah berikut dalam sembilan putaran:
    1. AddRoundKey: Mengombinasikan state dengan round key menggunakan XOR.
    2. InvMixColumns: Mengalikan setiap kolom state dengan matriks AES untuk mengembalikan data ke bentuk aslinya.
    3. InvShiftRows: Melakukan pergeseran kembali baris pada state.
    4. InvSubBytes: Mengubah elemen state kembali menggunakan S-Box.
e. Final Round: Pada ronde terakhir, langkah InvMixColumns tidak dilakukan. Setelah menyelesaikan

semua putaran:

1. AddRoundKey: Mengombinasikan state terakhir dengan round key.

f. Hasil: Proses dekripsi menghasilkan plaintext yang merupakan data asli sebelum dienkripsi.

1.10 Jadwal Penelitian

Adapun jadwal dari penelitian yang dilakukan adalah sebagai berikut :

Tabel 1. 1 Jadwal penelitian

Kegiatan	Bulan																			
	Oktober				November				Desember				Januari				Februari			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Penyusunan Proposal																				
Requirements Planning																				
Seminar Usulan Proposal																				
User Design																				
Construction																				
Cutover																				
Seminar Hasil Proposal																				
Sidang Akhir																				

1.11 Sistematika Penelitian

BAB I : PENDAHULUAN

Pada bab ini menjelaskan tentang tentang Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan dan Manfaat, Metodologi Penelitian,Teknik Pengumpulan Data, Lokasi Penelitian, dan Sistematika Penulisan.

BAB II : LANDASAN TEORITIS

Bab ini memuat tentang teori dasar yang berhubungan dengan program yang dirancang, serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN PERANCANGAN

Bab ini menjelaskan tentang analisis permasalahan yang sedang berjalan, serta memuat tentang analisis sistem dan perancangan sistem yang akan dibuat.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

Bab pengujian dan implementasi ini, membahas hasil-hasil dari tahapan penelitian, analisis, desain, implementasi desain, hasil pengujian dan implementasi. Hasil pengujian (testing) program menggunakan pengujian kotak hitam (Black-box testing), kotak putih (White-box testing) dan User Acceptance Testing (UAT) di mana pengguna akhir (pimpinan, kasir, pelanggan, dan koki).

BAB V : KESIMPULAN DAN SARAN

Bab ini memuat kesimpulan dari apa yang telah dibuat sebelumnya dan saran yang ditunjukan baik kepada ilmu pengetahuan atau kepada masyarakat luas untuk dapat melakukan penelitian yang lebih lanjut.