BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebuah bisnis di bidang makanan, Cafe Siang Malam"7" 24 Jam adalah tempat penyedia makanan dan minuman cepat saji dan menyuguhkan suasana santai atau tidak resmi. Dirintis sejak 2007 dan dibangun di tempat yang strategis menjadi pondasi yang kuat untuk perkembangan bisnis makanan. Perhitungan matang mengenai aspek pengadaan bahan baku yang pasti, kualitas makanan yang terjaga baik, finansial yang matang, harga yang terjangkau, kenyamanan, operasional yang terkontrol serta *marketing* yang tajam dan jitu menciptakan segmentasi pasar yang luas semakin meluruskan usaha Café Siang Malam "7" 24 Jam. Dengan begitu bisnis ini akan menjadi bisnis yang potensial untuk berkembang dan memiliki prospek yang bagus untuk ke depannya. Dengan prospek yang bagus maka akan memberikan keuntungan yang semakin besar untuk jangka panjang.

Hasil dari wawancara dengan pemilik kafe, Cafe Siang Malam "7" 24 Jam merupakan usaha penyedia makanan dan minuman cepat saji, yang berlokasi di daerah Grogol Petamburan, Kota Jakarta Barat. Sistem pemesanan yang digunakan oleh Cafe Siang Malam "7" 24 Jam masih menggunakan sistem dengan mencatat menu makanan dan minuman yang dipesan pelanggan oleh pelayan menggunakan kertas. Dengan sistem yang masih digunakaan saat ini, karena belum memanfaatkan teknologi sistem informasi, pelanggan harus menunggu giliran untuk dilayani oleh pelayan yang jumlahnya terbatas dalam melakukan pemesanan sehingga mengakitbatkan terjadinya penumpukan pemesanan dan membutuhkan waktu yang lama. Selain itu, pesanan yang dicatat pada lembar kertas, sering terjadinya ketidaksesuaiaan pesanan pelanggan dengan jumlah nomimal yang harus dibayarkan karena kecurangan pelanggan yang tidak bertanggung jawab. Dimana jumlah pemesanan yang lebih banyak dari pesanan yang diminta oleh pelanggan dan harga yang tidak sesuai dengan

yang ada di menu, sehingga jumlah nominal yang harus dibayar lebih besar dari yang seharusnya. Kejadian ini berdampak pada kepercayaan pelanggan dengan menurunnya jumlah pelanggan yang datang ke Cafe Siang Malam "7" sehingga mengakibatkan turunnya income/pemasukan dan dapat merusak nama baik bagi Cafe Siang Malam "7".

Untuk mengatasi permasalahan diatas dibutuhkan sebuah sistem atau aplikasi sebagai solusi. Oleh karena itu, peneliti membangun sebuah aplikasi pemesanan makanan dengan QR-Code di Cafe Siang Malam "7" 24 Jam dengan menerapkan algoritma Rijndael untuk proses kriptografi sebagai keamanan data transaksi.

Kriptografi adalah teknik untuk memastikan kerahasiaan dan keamanan pesan saat dikirim ke tujuan, mencegah penyadapan. Enkripsi, dekripsi, dan kunci adalah tiga dasar kriptografi. Fungsi utama kriptografi adalah merahasiakan kunci dan mengubah plaintext menjadi ciphertext, sehingga plaintext menjadi password yang tidak diketahui orang lain, tanpa harus merahasiakan algoritma yang digunakan. Jika kata sandi digunakan untuk kerahasiaan dan keamanan dapat dibaca oleh orang lain, maka kerahasiaannya terancam [1].

Cyber crime adalah tindak kejahatan yang dilakukan dengan memanfaatkan teknologi komputer sebagai alat kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet [2]. Data sensitif harus dilindungi, termasuk data transaksi pengguna. Data transaksi tersebut merupakan data pembayaran yang bersifat rahasia dan harus dilindungi untuk mencegah penyalahgunaan data. Oleh karena itu, diperlukan suatu algoritma yang dapat mengenkripsi data sensitif sedemikian rupa sehingga pengguna tanpa hak akses tidak dapat mengetahui isi data tersebut[3].

Algoritma yang digunakan untuk proses enkripsi pada penelitian ini adalah Algoritma Rijndael. Rijndael dikembangkan oleh 2 ahli kriptografi yang berasal dari Belgia yaitu Joan Daemen dan Vincent Rijmen. Pada tahun 1997, National Institute of Standard and Technology (NIST)

mengadakan sebuah kompetisi untuk membuat algoritma enkripsi Advanced Encryption Standard (AES). Kompetisi ini diadakan untuk menggantikan standar enkripsi yang sebelumnya, Data Encryption Standard (DES) yang telah ditemukan celah-celah untuk dilakukannya kriptoanalisis. Algoritma AES menggunakan block cipher dengan ukuran minimal blok 128 bit, serta mendukung 3 ukuran kunci, yaitu 128 bit, 192 bit, dan 256 bit. Pada tanggal 9 Agustus 1999, NIST melalui seleksi yang sangat ketat mengumumkan 5 finalis yang akan memasuki seleksi akhir yaitu MARS, RC6, Rijndael, Serpent, dan Twofish. Pada seleksi akhir tanggal 2 Oktober 2000 maka terpilihlah Rijndael sebagai pemenang. Algoritma Rijndael dibuat oleh Dr. Vincent Rijmen dan Dr. Joan Daemen. Algoritma Rijndael atau yang sekarang lebih dikenal sebagai AES, ialah algoritma block cipher yang menggunakan sistem subtitusi (S-Box). AES tergolong dalam symmetric encryption dikarenakan hanya memerlukan satu key untuk melakukan enkripsi maupun dekripsi [4]. Keseluruhan kunci dari Rijndael cukup untuk melindungi data yang ada didalamnya. Rijndael termasuk kedalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Oleh karena itu, algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

QR Code adalah kode batang dua dimensi yang merupakan pengembangan barcode barcode sebelumnya. Jika data barcode lama disimpan secara horizontal, tetapi QR Code data disimpan secara horizontal dan vertikal. Dengan kemampuan untuk menyimpan dalam dua dimensi QR Code tentunya bisa menyimpan lebih banyak data dan variatif daripada barcode. Itu jenis data yang dapat disimpan di QR Code adalah termasuk mode Numerik, mode Alfanumerik, 8- bit mode byte, dan Mode Kanji [5].

Dampak penggunaan teknologi smartphone dirasakan dalam banyak hal, setiap restoran dan kafe ingin memanfaatkan teknologi smartphone untuk kepuasan pelanggan dan untuk kepentingan pihak restoran. Manusia pada umumnya menginginkan segala sesuatu dapat dengan mudah

dikerjakan, begitu pula dengan pelanggan restoran yang ingin memesan menu dengan mudah, dalam artian tidak rumit dan tidak memakan waktu yang lama. Mudah dalam memesan menu yang dimaksud adalah tanpa harus mengantri dan tanpa harus menunggu pelayan yang sibuk dengan pelanggan lainnya. Pelanggan restoran juga dapat mengambil waktu dalam memesan pesanan yang sesuai kebutuhan sehingga tidak terganggu dengan keberadaan pelayan yang sedang menunggu pesanan tersebut [6].

Meningkatnya persaingan bisnis antar penyedia layanan ataupun pengguna layanan, serta didukung oleh meningkatnya kemampuan pengguna komputer menjadikan banyak pemakai mencoba-coba membongkar, bahkan sengaja menjatuhkan kinerja aplikasi lawan bisnis. *Security* menjadi isu utama dalam pengembangan teknologi keamanan transaksi online. Resiko kebocoran data baik akibat dari kesalahan manusia, maupun kegagalan sistem dalam menangani ancaman berakibat pada kerugian material maupun sosial, serta tidak jarang berakhir pada kasus hukum. Kemanan dalam dunia internet mengacu pada rumusan standar ISO IEC 270002 2005 (ISO IEC 17799 2005). Dalam standar tersebut dijelaskan bahawa salah satu bentuk dari pengelolaan resiko aset informasi adalah dengan menyusun dan menerapkan kebijakan keamanan informasi, terutama dalam keamanan data dalam sistem informasi, khususnya data transaksi online. Penerapan metode enkripsi pada data pelanggan dapat menjadi salah satu solusi pencegahan penyalahgunaan data[7].

Pengamanan informasi dilakukan dengan metode kriptografi dengan cara mengubahnya dalam bentuk yang rumit dan sulit dibaca [8]. Enkripsi dan dekripsi digunakan dalam metode ini. Enkripsi merupakan proses mengamankan data yang dapat dibaca (plaintext) menjadi data yang rumit untuk dibaca (ciphertext) sedangkan dekripsi adalah mengembalikkan data yang rumit untuk dibaca (ciphertext) menjadi data yang mudah dibaca (plaintext).

Berdasarkan uraian pada latar belakang dan kondisi yang sudah dijelaskan, perlu adanya penelitian guna menemukan solusi untuk masalah diatas dan mampu memaksimalkan sumber daya yang sudah tersedia. Oleh

karena itu, peneliti berusaha merancang serta membangun sistem perangkat lunak berdasarkan algoritma Rijndael yang dapat digunakan untuk proses kriptografi sebagai kemanan data transaksi. Maka dari itu penulis akan melakukan penelitian dengan judul "**Rancang Bangun Aplikasi Pemesanan Makanan Dengan QR Code di Café Siang Malam "7" 24 Jam menggunakan Algoritma Rijndael**".

1.2 Identifikasi Masalah

Berdasarkan permasalahan yang ada dari latar belakang diatas, peneliti dapat mengidentifikasi masalah antara lain :

1. Pesanan yang dicatat pada lembar kertas, sering terjadinya ketidaksesuaiaan pesanan pelanggan dengan jumlah nominal yang harus dibayarkan karena kecurangan pelanggan yang tidak bertanggung jawab.
2. Data transaksi berisi data pesanan dan informasi pembayaran perlu diamankan untuk menghindari penyalahgunaan data seperti manipulasi data pada jumlah pesanan dan kesalahan perhitungan pada total pembayaran yang berdampak pada kepercayaan pelanggan dan mengakibatkan turunnya income/pemasukan bagi cafe serta dapat merusak nama baik cafe.

1.3 Rumusan Masalah

Dalam uraian latar belakang permasalahan, adapun rumusan masalahnya adalah :

1. Bagaimana merancang bangun aplikasi pemesanan makanan dengan QR-Code untuk mempermudah pengelolaan data pesanan pelanggan di Cafe Siang Malam “7” 24 Jam?
2. Bagaimana menerapkan algoritma Rijndael pada aplikasi pemesanan makanan untuk meminimalisir terjadinya kecurangan di Cafe Siang Malam “7” 24 Jam?

1.4 Batasan Masalah

Untuk memudahkan pemecahan masalah perlu dilakukan pembatasan sehingga permasalahan menjadi lebih sederhana. Batasan masalah tersebut meliputi :

1. Penelitian dilakukan di Cafe Siang Malam “7” 24 Jam.
2. Penelitian ini ditujukan untuk pembuatan aplikasi keamanan pada data pesanan.
3. Algoritma Rijndael :

a. Algoritma yang digunakan pada penelitian untuk proses enkripsi dan deskripsi adalah Rijndael .
b. Data yang dienkripsi adalah id pesanan.
c. Id pesanan terdiri dari angka dan huruf
d. Informasi yang akan ditampilkan dari QR-Code yang telah didekripsi adalah detail transaksi yang terdiri dari nama pelanggan, data pesanan, jenis pesanan, dan total pembayaran.

4. Aplikasi yang dibangun
   a. Entitas pada aplikasi ini terdiri dari Pelanggan (*Customer*) sebagai *user,* Pemilik (Pemilik), Kasir, Koki, dan *Kurir*.
   b. Hak akses dari masing-masing Entitas adalah sebagai berikut :
      1) *Customer* yaitu dapat melihat daftar menu, melakukan pemesanan (*dine in, takeaway* atau *delivery)*, mengedit pesanan, melihat status pesanan dan melakukan transaksi.
      2) Kasir dapat mengelola status data pesanan untuk pembayaran
      3) Koki dapat melihat data pesanan dan update status pesanan serta dapat update ketersediaan menu.
      4) Pemilik (Pemilik) memiliki akses untuk dapat melihat hak akses dari entitas kasir dan koki. Pemilik (Pemilik) juga memiliki hak akses tersendiri yaitu mengelola data daftar menu seperti tambah, edit, hapus menu dan dapat melihat rekap laporan penjualan.
      5) Kurir dapat mengelola status data pesanan untuk pembayaran dan mengupdate status pesanan.
   c. Aplikasi yang diakses oleh Pemilik dan customer dibangun dengan aplikasi frontend dan backend menggunakan Bahasa Pemrograman PHP dengan *database MySQL*.
   d. Tools yang digunakan untuk membangun aplikasi ini adalah Visual Studio Code, XAMPP, Web Browser, Microsoft Visio, dan Star Uml.

1.5 Tujuan Penelitian

Berdasarkan permasalah yang ada pada rumusan diatas, maka tujuan yang hendak dicapai dari penelitian yaitu :

1. Merancang bangun aplikasi pemesanan menu untuk meminimalisir kecurangan pemesanan di Cafe Siang Malam “7” 24 Jam.
2. Mengimplementasikan algoritma Rijndael pada aplikasi pemesanan makanan untuk proses enkripsi dan deskripsi pada data pesanan di Cafe Siang Malam “7” 24 Jam.

1.6 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberi manfaat bagi beberapa pihak terkait proses yang dilaksanakan, adalah sebagai berikut :

1. Manfaat Teoritis

   Secara teoritis penelitian ini diharapkan dapat bermanfaat yaitu :

   a. Menambah pengetahuan bagi peneliti tentang pembuatan dan penerapan QR-Code.
   b. Menambah wawasan bagi peneliti mengenai kriptografi dan Algoritma Rijndael.
2. Manfaat Praktis

   Secara praktis penelitian ini diharapkan dapat bermanfaat yaitu :

   a. Bagi Cafe Siang Malam “7” 24 Jam
      1) Dapat mempermudah dalam mengelola data menu, data pesanan, dan data pembayaran.
      2) Mengurangi penumpukan kertas pesanan dan meminimalisir kesalahan pencatatan dalam pemesanan.
      3) Memudahkan pemilik untuk melihat rekapitulasi penjualan.
   b. Bagi Pelanggan
      1) Dapat memudahkan Pelanggan dalam melakukan pemesanan menu.
      2) Dapat mengamankan data pesanan Pelanggan.

1.7 Pertanyaan Penelitian

Berdasarkan penelitian ini ada beberapa pertanyaan yang terkait dengan penelitian yang dilakukan. Adapun pertanyaan penelitian tersebut :

1. Apakah dapat merancang bangun aplikasi pemesanan makanan dengan QR-Code untuk meminimalisir terjadinya ketidaksesuaiaan pesanan pelanggan dengan jumlah nominal yang harus dibayarkan di Cafe Siang Malam “7” 24 Jam ?
2. Apakah dapat menerapkan algoritma Rijndael pada aplikasi pemesanan makanan di Cafe Siang Malam “7” 24 Jam untuk proses enkripsi dan deskripsi pada data pesanan ?

1.8 Hipotesis Penelitian

Berdasarkan hasil pemaparan yang dijelaskan diatas, maka dapat dikemukakan hipotesis “Dengan dibangunnya aplikasi pemesanan makanan dengan *QR-Code* di Café Siang Malam “7” 24 Jam menggunakan algoritma *Rijndael*, diharapkan dapat mempermudah dalam pemesanan menu serta dapat mengamankan data pesanan di Cafe Siang Malam “7” 24 Jam.

1.9 Metodologi Penelitian

Metodologi penelitian yang digunakan peneliti meliputi beberapa metode, yaitu metode pengumpulan data dan metode pengembangan sistem. Pembahasan metode-metode tersebut adalah:

1.9.1 Metode Pengumpulan Data

a. Studi Pustaka

Studi Pustaka dilakukan dengan cara mengumpulkan data yang diarahkan untuk mendapatkan sumber informasi seperti jurnal yang bersifat ilmiah mengenai pelayanan pemesanan, pengamanan data, Algoritma Rijndael, *QR-Code* dan juga yang lainnya yang berkaitan dengan penelitian.

b. Observasi

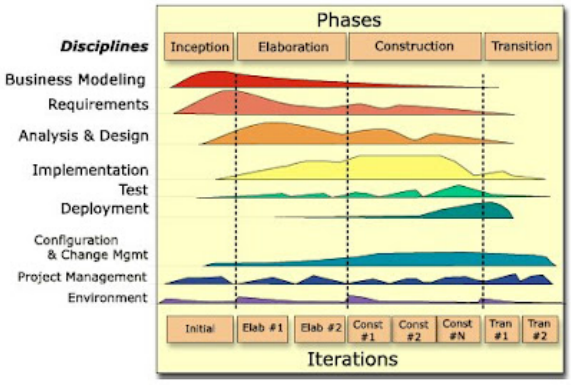
Observasi untuk pengumpulan data dilakukan dengan cara meninjau langsung ke Objek yang akan diteliti. Untuk mendapatkan data yang bersifat nyata dan meyakinkan penulis melakukan pengamatan langsung pada Café Siang Malam "7" 24 Jam.

c. Wawancara

Dalam Wawancara ini, peneliti mengumpulkan data penelitian dengan bertanya langsung kepada pemilik Café Siang Malam "7" 24 Jam yang dapat memberikan informasi yang dibutuhkan.

1.9.2 Metode Pengembangan Sistem

Dalam pengembangan sistem ini menggunakan metode RUP (*Rational Unified Process*). RUP merupakan pendekatan pengembangan perangkat lunak yang dilakukan secara iterative (berulang) dan incremental (bertahap dalam progres menarik) dimana setiap iterasi akan memperbaiki iterasi berikutnya, serta proses rekayasa perangkat lunak yang baik (*well-structure*) dan mempunyai penstrukturan yang baik (*well-structured*) [6]. Berikut adalah gambar dari tahapan dalam *Rational Unified Process* dapat dilihat pada Gambar 1.



Gambar 1.1 Metode Pengembangan Sistem RUP

Tahapan RUP dijelaskan sebagai berikut :

1. *Inception* (Permulaan)

   Pada tahapan permulaan ini berfokus pada permodelan proses bisnis yang akan dibutuhkan dan mendefinisikan kebutuhan dari sistem yang akan dikembangkan. Dengan menggunakan data yang diambil dari hasil wawancara dan observasi dari hasil penelitian yang dilakukan oleh peneliti [9].

   a. *Bussines Modelling*, pada tahapan ini peneliti membuat flowmap sistem yang sedang berjalan.
   b. *Requirements*, pada tahapan ini peneliti melakukan identifikasi kebutuhan fungsional dan non-fungsional dari sistem yang akan dibuat.
   c. *Analysis & Design*, pada tahapan ini peneliti membuat flowmap sistem usulan.
   d. *Implementation*, pada tahapan ini dilakukan pemilihan spesifikasi minimum device yang dibutuhkan untuk menjalankan sistem.
   e. *Test*, pada tahapan ini dilakukan proses mengidentifikasi pengujian apa saja yang akan dilakukan.
   f. *Configuration & Change Management*, pada tahapan ini dilakukan proses konfigurasi sistem yang bertujuan untuk mengelola perubahan yang mungkin terjadi.
   g. *Project Management*, pada tahapan ini dilakukan proses pemantauan kemajuan dari pengembangan sistem.
   h. *Environment*, pada tahapan ini dilakukan proses penyediaan lingkungan pengembangan sistem dengan memastikan perangkat lunak yang diperlukan tersedia.

2. *Elaboration* (Perancanaan)

   Elaboration merupakan tahap untuk melakukan desain secara lengkap berdasarkan hasil analisis yang berfokus pada prototype. Tahapan ini merupakan pembuatan desain arsitektur sistem yang

di usulkan, desain format data, desain database desain tampilan.

a. *Business Modelling*, pada tahapan ini dilakukan pembuatan use case diagram, scenario usecase, class diagram, activity diagram, class diagram, dan sequence diagram.
b. *Requirements*, pada tahapan ini dilakukan perincian dari kebutuhan fungsional dan non fungsional dengan lebih detail.
c. *Analysis & Design*, pada tahapan ini dilakukan pembuatan wireframe dari sistem yang akan dibuat.
d. *Implementation*, pada tahapan ini mulai dilakukan penulisan kode program dengan bahasa pemrograman PHP dengan database MYSQL untuk aplikasi admin.
e. *Test*, pada tahapan ini dilakukan pengujian untuk memastikan alur sistem berjalan sesuai harapan dan tidak ada error, jika kode program ditemukan error maka dilakukan perbaikan pada kode program.
f. *Deployment*, pada tahapan ini memastikan jika ada perubahan pada perangkat lunak yang sedang dibangun dapat diimplementasikan dengan baik.
g. *Configuration & Change Management*, pada tahapan ini dilakukan pengelolaan pada perubahan yang muncul selama di 14 fase elaboration kemudian dilakukan konfigurasi untuk memastikan konsistensi.
h. *Project Management*, pada tahapan ini dilakukan pemantauan pengembangan proyek sistem.
i. *Environtment*, pada tahapan ini dilakukan proses menyempurnakan dan memelihara lingkungan pengembangan dan pengujian dengan memastikan dan menyediakan kebutuhan infrastruktur terpenuhi.

3. *Construction* (Konstruksi)

   Pengimplementasian rancangan perangkat lunak yang telah

dibuat dilakukan pada tahap ini. Apabila desain yang dibuat telah sesuai dengan analisis sistem, maka implementasi dengan bahasa pemrograman tertentu dapat dilakukan. Pada penelitian ini sistem dibangun menggunakan Bahasa Pemrograman PHP untuk user pelanggan, pemilik, koki, kasir dan kurir. Dan database menggunakan MySQL. Kemudian dilakukan *test* dengan *blackbox testing* dan *whitebox testing* untuk memastikan aplikasi berjalan dengan baik. Test digunakan untuk memastikan interaksi dan integrasi antar objek, seluruh kebutuhan terpenuhi dan mengidentifikasi kekurangan. *Blackbox Testing* dan *Whitebox Testing* dilakukan pada tahap ini untuk memastikan aplikasi berjalan dengan baik.

a. *Business modelling*, pada tahapan ini dilakukan penyempurnaan dan pembaruan model bisnis berdasarkan perubahan yang ada.
b. *Requirement*, pada tahapan ini dilakukan pengelolaan perubahan kebutuhan yang mungkin ada selama implementasi.
c. *Analisys & design*, pada tahapan ini dilakukan analisis terhadap desain wireframe yang telah dibuat, dan dilakukan perbaikan terhadap perubahan yang ada.
d. *Implementation*, pada mengimplementasikan tahapan ini komponen-komponen peneliti sistem berdasarkan desain yang telah dibuat, melakukan penulisan kode program untuk fitur baru atau perubahan yang diperlukan.
e. *Test*, pada tahapan ini peneliti melakukan pengujian aplikasi dengan menggunakan uji blackbox, dan uji whitebox.
f. *Deployment*, pada tahapan ini peneliti menanggapi masalah yang muncul selama atau setelah implementasi.
g. *Configuration & Change Management*, pada tahapan ini dilakukan pengelolaan perubahan yang mungkin muncul.

h. *Project Management*, pada tahapan ini dilakukan proses identifikasi dan menganggapi risiko yang muncul selama fase construction.
i. *Environment*, pada tahapan ini dilakukan proses pemeliharaan dan pengelolaan lingkungan pengembangan dan pengujian, serta memastikan infrastruktur dan sumber daya memadai.

4. *Transition* (Transisi)

Pada tahap transisi, dilakukan implementasi dan pengujian dari sistem yang telah dibuat, melakukan instalasi sistem agar dapat dimengerti dan digunakan oleh pengguna. Menghasilkan produk perangkat lunak yang menjadi syarat dari batas kemampuan operasional awal termasuk pada pelatihan user, pemeliharaan, dan pengujian sistem apakah sudah memenuhi harapan user. *Deployment* Tahap ini merupakan proses memproduksi rilis perangkat lunak dan pelatihan kepada pengguna sehingga siap digunakan dan didistribusikan.

a. *Business Modelling*, pada tahapan ini dilakukan penyempurnaan dan pembaruan model bisnis berdasarkan perubahan yang ada.
b. *Requirements*, pada tahapan ini dilakukan verifikasi dan validasi terakhir terhadap kebutuhan.
c. *Analysis & Design*, pada tahapan ini dilakukan evaluasi dan verifikasi terhadap desain yang telah diimplementasikan.
d. *Implementation*, pada tahapan ini memastikan alur kerja sistem yang diimplementasikan berfungsi seperti yang direncanakan.
e. *Test*, pada tahapan ini dilakukan pengujian aplikasi dengan uji UAT (User Acceptance Testing) oleh konsumen sebanyak 30 responden.
f. *Deployment*, pada tahapan ini dilakukan proses

pengaplikasian sistem kepada *user*.

g. *Configuration & Change Management*, pada tahapan ini dilakukan penanganan terhadap perubahan yang terjadi selama fase transition.
h. *Project Management*, pada tahapan ini dilakukan peninjauan akhir pada proyek, dan menilai kesesuaian proyek dengan tujuan dan kebutuhan awal.
i. *Environment*, pada tahapan ini dilakukan proses evaluasi dan pembaruan terakhir pada lingkungan pengembangan dan pengujian sistem.

1.9.3 Metode Penyelesaian Masalah

Rijndael merupakan jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit [10]. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Berikut adalah perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan.

Tabel 1. 1 Ukuran Blok dan Jumlah Proses

	Ukuran Blok Data (Nb) Dalam Words	**Jumlah proses (Nr)**
128 – bit	4	10
192 – bit	4	12
256 – bit	4	14

1.9.3.1 Proses Sub Kunci (*Key Schdule*)

Proses key schedule diperlukan untuk mendapat beberapa sub kunci dari kunci utama agar cukup untuk melakukan enkripsi dan

dekripsi. Proses untuk mendapatkan sub kunci dilakukan setelah state dikonversi kedalam bentuk hexadecimal, dengan menggukan tabel ASCII.

Tabel 1. 2 Tabel ASCII

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	@	96	0110 0000	60	`
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22	"	66	0100 0010	42	B	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	c
4	0000 0100	04	[EOT]	36	0010 0100	24	$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	%	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	&	70	0100 0110	46	F	102	0110 0110	66	f
7	0000 0111	07	[BEL]	39	0010 0111	27	'	71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	08	[BS]	40	0010 1000	28	(	72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29	)	73	0100 1001	49	I	105	0110 1001	69	i
10	0000 1010	0A	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	l
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	M	109	0110 1101	6D	m
14	0000 1110	0E	[SO]	46	0010 1110	2E	.	78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	O	111	0110 1111	6F	o
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	S	115	0111 0011	73	s
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	V	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	W	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	X	120	0111 1000	78	x
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	y
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	Z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[	123	0111 1011	7B	{
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	|
29	0001 1101	1D	[GS]	61	0011 1101	3D	=	93	0101 1101	5D	]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3F	?	95	0101 1111	5F	_	127	0111 1111	7F	[DEL]

Penjelasan operasi key schedule yaitu sebagai berikut :

1. Operasi Rotate, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
2. Operasi SubBytes, pada operasi ini 8 bit dari subkey disubtitusikan dengan nilai dari S-Box.

Tabel 1. 3 Rijndael S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

3. Operasi Rcon, operasi ini diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari user. Operasi ini menggunakan nilai-nilai dalam *Galois Field*. Nilai – nilai dari Rcon kemudian akan di XOR dengan hasil SubBytes.

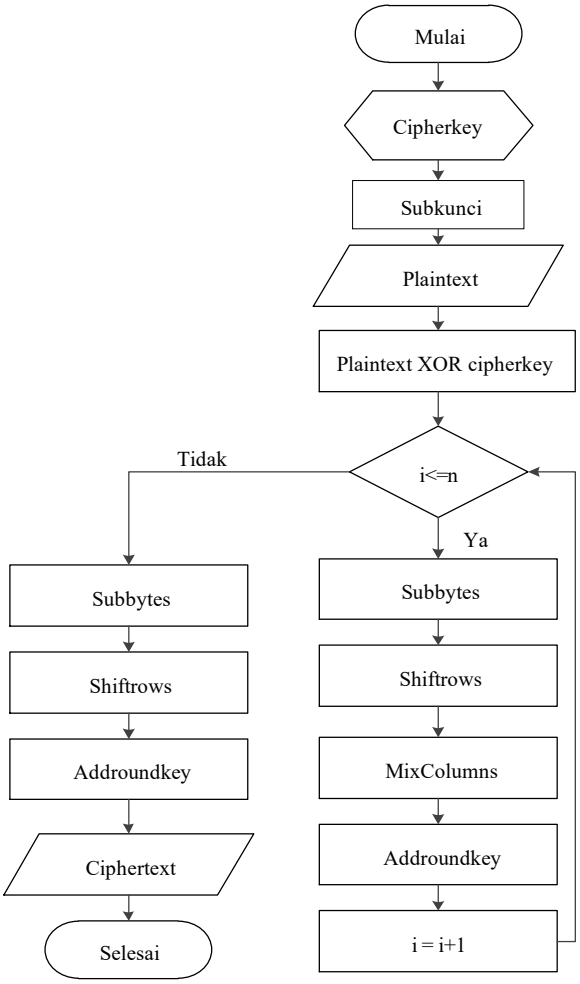
Tabel 1. 4 Tabel Rcon

Rcon [1]	Rcon [2]	Rcon [3]	Rcon [4]	Rcon [5]	Rcon [6]	Rcon [7]	Rcon [8]	Rcon [9]	Rcon [10]
01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

4. Operasi XOR dengan $w[i - Nk]$ yaitu word yang berada pada Nk sebelumnya.
5. Proses perhitungan dilakukan 10 kali hingga mendapatkan 10 sub kunci.

1.9.3.2 Proses *Enkripsi*

Flowchart untuk proses Enkripsi pada algoritma Rijndael AES-128 bit dapat dilihat pada gambar 1.2 .



Gambar 1. 2 *Flowchart Enkrpsi* Rijndael AES – 128

Untuk proses enkripsi pada awalnya plainteks akan diubah ke representasi hexadesimal. Operasi yang dilakukan dalam proses enkripsi pada AES ada 4. yaitu AddRounKey, SubBytes, ShiftRows, dan MixColoumns. Kemudian, State akan transformasi secara berulang sebanyak Nr, pada proses ini disebut Round function. Pada Final Round, state tidak akan mengalami transformasi MixColoumns.

1. *AddRoundKey*

   Pada proses ini dilakukan XOR antara *state* dengan *round key* yang telah dibuat berdasarkan *chiper key*. Transformasi *AddRoundKey* diawali diawali dengan *round*=0 untuk *round* selanjutnya *round=round* +1. Pada proses deskripsi Transformasi

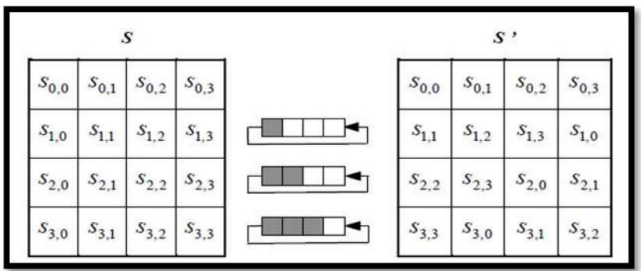
AddRoundKey diawali pada *round*=14 dan untuk *round* selanjutnya *round* = *round* – 1.

2. *SubBytes*

   Pada proses ini dilakukan penukaran tiap byte yang ada dalam blok state awal dengan yang ada pada Rijndael S-Box sehingga terbentuk sebuah blok baru yang akan digunakan sebagai state. [3]. Nilai subtitusi dinyatakan S`[r,c] yaitu elemen didalam tabel subtitusi yang merupakan perpotongan baris x dengan kolom y.

3. *ShiftRows*

   Pada proses ini dilakukan *shift* atau penggeseran elemen tiap barisnya. Pada baris pertama tidak dilakukan penggeseran. Pada baris kedua dilakukan satu kali penggeseran. Pada baris ketiga dilakukan dua kali penggeseran. Terakhir, pada baris keempat dilakukan tiga kali penggeseran. Penggeseran ini dilakukan ke arah kiri. Dapat dilihat Transformasi *ShiftRows* pada gambar 1.3 .



Gambar 1. 3 Transformasi Shiftrow

4. MixColumns

   MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada *state*.

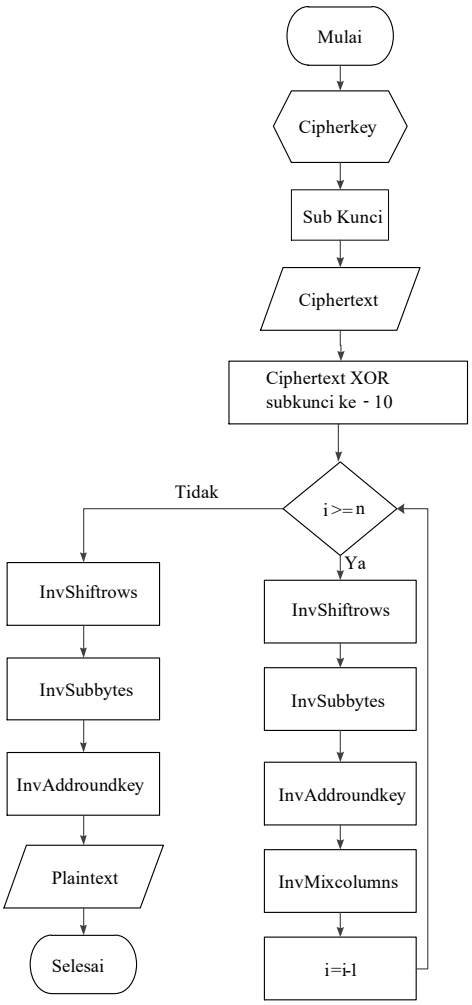
$$\begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

   Pada proses ini dilakukan perkalian blok dengan sebuah matriks.

$$s'_{0,c} = (\{02\} \bullet s_{o,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$
$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$
$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$
$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c})$$

1.9.3.3 Proses Dekripsi

Flowchart pada proses deskripsi pada algoritma Rijndael AES-128 bit dapat dilihat pada gambar 1.4 .

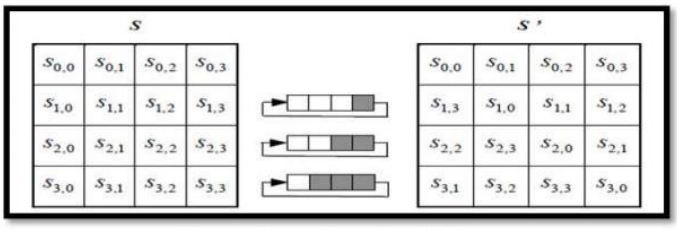


Gambar 1. 4 Flowchart Deskripsi Rijndael AES – 128

Transformasi byte yang digunakan dalam proses deskripsi ada 4, yaitu *InvShiftRows* ,*InvSubBytes* ,*InvAddRoundKey, InvMixColumns.*

1. *InvShiftRows*

   InvShiftRows sama seperti *ShiftRows* namun melakukan pergeseran dalam arah berlawanan yaitu ke kanan untuk tiap-tiap baris pada tiga baris terakhir di dalam *state*. Proses transformasi *InvShiftRows* dapat dilihat pada gambar 1.5 .



Gambar 1. 5 Transformasi InvShiftrows

2. *InvSubBytes*

   InvSubBytes adalah transformasi bytes yang berkebalikan dari transformasi *SubBytes*, tabel *S-Box* yang digunakan adalah tabel inversi dari *S-Box*. Tabel inversi S-Box dapat dilihat pada Tabel 1.5 .

Tabel 1.5 Inversi S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	B	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

3. *InvAddRoundkey*

   Pada proses ini dilakukan penggabungan sub kunci dengan hasil *InvSubBytes* menggunakan operasi XOR untuk setiap *Byte*.

4. *InvMixColumns*

Pada proses *InvMixColumns* merupakan proses mengalikan tiap kolom dalam *state* dengan matiks perkalian AES.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Hasil dari perkalian matriks adalah :

$$s'_{0,c} = (\{0E\} \bullet s_{o,c}) \oplus (\{0B\} \bullet s_{1,c}) \oplus (\{0D\} \bullet s_{2,c}) \oplus (\{09\} \bullet s_{3,c})$$
$$s'_{1,c} = (\{09\} \bullet s_{o,c}) \oplus (\{0E\} \bullet s_{1,c}) \oplus (\{0B\} \bullet s_{2,c}) \oplus (\{0D\} \bullet s_{3,c})$$
$$s'_{2,c} = (\{0D\} \bullet s_{o,c}) \oplus (\{09\} \bullet s_{1,c}) \oplus (\{0E\} \bullet s_{2,c}) \oplus (\{0B\} \bullet s_{3,c})$$
$$s'_{3,c} = (\{0B\} \bullet s_{o,c}) \oplus (\{0D\} \bullet s_{1,c}) \oplus (\{09\} \bullet s_{2,c}) \oplus (\{0E\} \bullet s_{3,c})$$

1.10 Jadwal Kegiatan

Adapun jadwal penelitian yang dilakukan dapat dilihat pada Tabel.

Tahapan Kegiatan	Agustus				September				November				Desember			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Inception (Permulaan)	■															
1. Melakukan Observasi		■	■													
2. Melakukan Wawancara		■	■													
Elaboration (Perencanaan)				■												
1. Flowchart				■												
2. Penggambaran UML					■											
3. Class Diagram					■											
4. Activity Diagram						■										
5. Use Case Diagram						■	■									
6. Sequence Diagram							■									
7. Perancangan Interface								■	■							
Construction (Konstruksi)										■						
1. Membuat Codingan										■	■	■	■			
2. Pengujian White Box														■		
3. Pengujian Black Box														■		
Transition (Transisi)															■	■

1.11 Sistematika Penulisan

BAB I : PENDAHULUAN

Bab ini berisi latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORITIS

Bab ini berisi tentang penjelasan dan semua materi yang digunakan dalam penyusunan skripsi.

BAB III : ANALISA DAN PERANCANGAN

Bab ini membahas tentang pembahasan dan penerapan semua unsur-unsur sistem yang telah dirancang dan dikembangkan.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi yang digunakan untuk mengaplikasikan perancangan baik mengetahui sejauh mana perangkat tersebut berguna dan bagaimana pengembangan berikutnya. Dari tahap tersebut kemudian dilanjutkan implementasi untuk menguji coba perangkat yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Bab ini merupakan bab terakhir dari penelitian, terdiri dari kesimpulan dan saran.