BAB III
METODE PENELITIAN

3.1 Tempat dan Waktu Penelitian

3.1.1 Tempat Penelitian

Adapun tempat peneliti melakukan penelitian dalam skripsi ini yaitu Laboratorium UINSU, Jl. IAIN No.1, Gaharu, Kec. Medan Tim., Kota Medan, Sumatera Utara 20235.

3.1.2 Waktu dan Jadwal Pelaksaan Penelitian

Waktu yang digunakan peneliti untuk penelitian ini dilaksanakan sejak tanggal dikeluarkannya ijin penelitian dalam kuran waktu bulan Juni s/d April 2022.

Tabel 3.1 Waktu dan Jadwal Penelitian

NO	Keterangan	Tahun 2021/2022										
		juni	July	Agust	Sep	Okt	Nov	Des	Jan	Feb	Mar	Apr
1	Pengumpulan Data	■	■	■								
2	Analisis Kebutuhan				■	■						
3	Perancangan Sistem						■	■	■			
4	Penerapan									■	■	■

3.2Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam pembahasan penelitian ini adalah sebagai berikut:

1. Studi Literatur

   Merupakan tahap pengumpulan data dengan cara mengumpulkan literatur, jurnal, *paper*, dan buku-buku yang berkaitan dengan judul penelitian, serta mencari informasi dari berbagai sumber di internet untuk mengetahui perkembangan terbaru dari data yang diambil sebagai bahan dalam pembuatan tugas akhir.

2. Analisis dan perancangan sistem

   Tahap ini akan dilaksanakan analisa data, kebutuhan sistem yang digambarkan dalam *flowchart*, dan perancangan antarmuka.

3. Implementasi sistem

Implementasi dilaksanakan berdasarkan hasil analisa dan perancangan yang telah dilakukan sebelumnya. Dalam tahap ini dilakukan pengkodean (*coding*) dalam menggunakan bahasa pemograman PHP.

4. Pengujian sistem

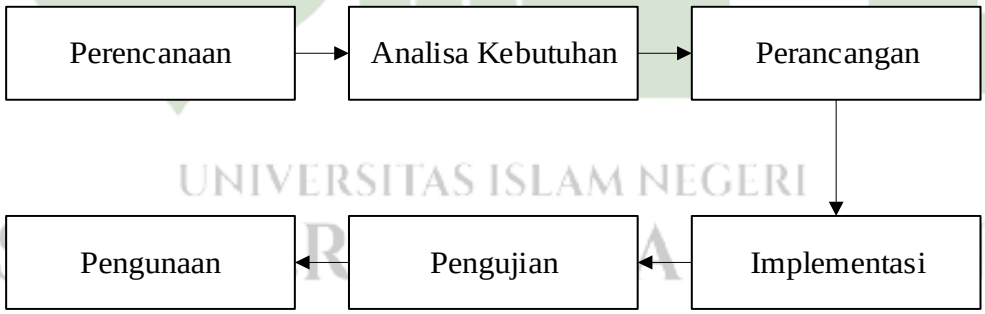
   Pengujian ini dilakukan pengujian terhadap proses kriptografi pada sistem yang telah di bangun. Meliputi input file pdf, proses enkripsi, proses dekripsi dan juga mencakup apakah implementasi sistem sudah sesuai dengan teori serta perancangan yang sudah dilakukan sebelumnya.

5. Hasil Pengujian Sistem

   Membuat hasil pengujian sistem, apakah sistem dapat menghasilkan keamanan file PDF sesuai dengan tujuan penelitian

3.3 Model Penelitian

Penelitian ini bertujuan untuk mengembangkan produk aplikasi keamanan data dokumen pdf dengan teknik kriptografi berbasis web. Penelitian ini termasuk ke dalam penelitian *Research and Development* (R & D). Metode penelitian ini digunakan untuk menghasilkan produk tertentu dan mengkaji keefektifan produk tersebut. *Research and Development* (R & D) merupakan suatu proses atau langkah-langkah untuk mengembangkan suatu produk baru atau menyempurnakan produk yang telah ada yang dapat dipertanggung jawabkan. Secara garis besar, langkah-langkah dalam model penelitian ini meliputi perencanaan (*planning*), analisa kebutuhan, perancangan, implementasi, pengujian dan penggunaan. Keenam langkah tersebut dapat dilihat dari bagan berikut ini:



Gambar 3.1 Bagan Langkah Penelitian

3.3.1 Perencanaan

Perencanaan penelitian ini meliputi dari pengumpulan data penelitian, melakukan anlisis kebutuhan sistem, melakukan perancangan sistem yang akan dibangun serta menguji sistem yang telah dibangun untuk memperoleh hasil dan kesimpulan.

3.3.2Analisa Kebutuahan

Pada penelitian ini bahan yang digunakan adalah file data dokumen dengan format *.pdf*. Sedangkan analisa kebutuhan meliputi perangkat keras (*hardware*) dan perangkat lunak (*software*).

1. Perangkat Keras

Adapun kebutuhan perangkat keras (*hardware*) yang digunakan penulis untuk mendukung penelitian adalah laptop dengan spesifikasi sebagai berikut :

Tabel 3.2 Kebutuhan *Hardware*

Nama Komponen	Spesifikasi
Procesor	ntel(R) Core i3
Memory	4GB
Harddisk	00 GB
Monitor	4 inchi

2. Perangkat Lunak

Adapun kebutuhan perangkat lunak (*software*) penulis yang digunakan untuk perancangan Aplikasi pengaman data dokumen PDF adalah sebagai berikut:

a. *XAMPP* untuk *Apache* dan *MySQL*
b. *Web Browser google crome* atau *Mozilla*

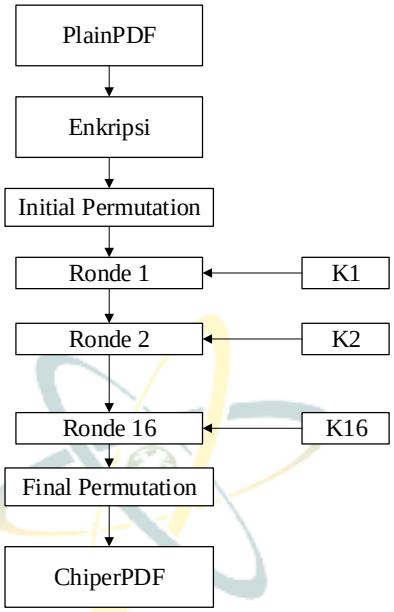
3.3.3 Perancangan

Perancangan sistem dalam suatu penelitian adalah tahap yang dilakukan peneliti setelah mengumpulkan semua kebutuhan sistem yang akan dirancang. Adapun form perancangan sistem aplikasi keamanan file PDF terdiri dari menu enkripsi dan dekripsi. Menu enkripsi adalah menu yang digunakan oleh user untuk melakukan proses pengamanan file PDF dengan algoritma DES, pada menu ini user dapat memilih file PDF yang ingin diamankan, kemudian memasukan kunci enskripsi, sedangkan menu dekripsi adalah menu yang digunakan oleh user untuk mengembalikan file PDF yang telah diamankan kedalam bentuk semula, pada for, ini user memasukan file PDF hasil enkripsi kemudian memasukan kunci deklripsi yang sama ketika proses enkripsi. Adapun berikut adalah racangan diagram enkrip dan dekripsi menggunakan algoritma DES:

1. *Diagram*Enkripsi Algoritma DES

Proses enkripsi dilakukan sebanyak 16 ronde. Tahap pertama dilakukan dengan proses *initial permutation*, kemudian proses ronde 1 hingga ronde 16, hasil ronde 16 diproses

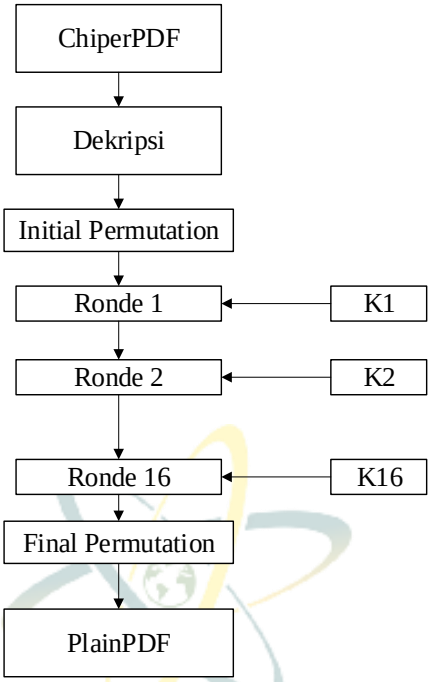
kembali dengan teknik *final permutation*, sehingga menghasilkan *chiperpdf*. Diagram enkripsi algoritma DES pada *plainpdf* sebagai berikut:



Gambar 3.2 Diagram Enkripsi DES

2. *Diagram*Dekripsi Algoritma DES

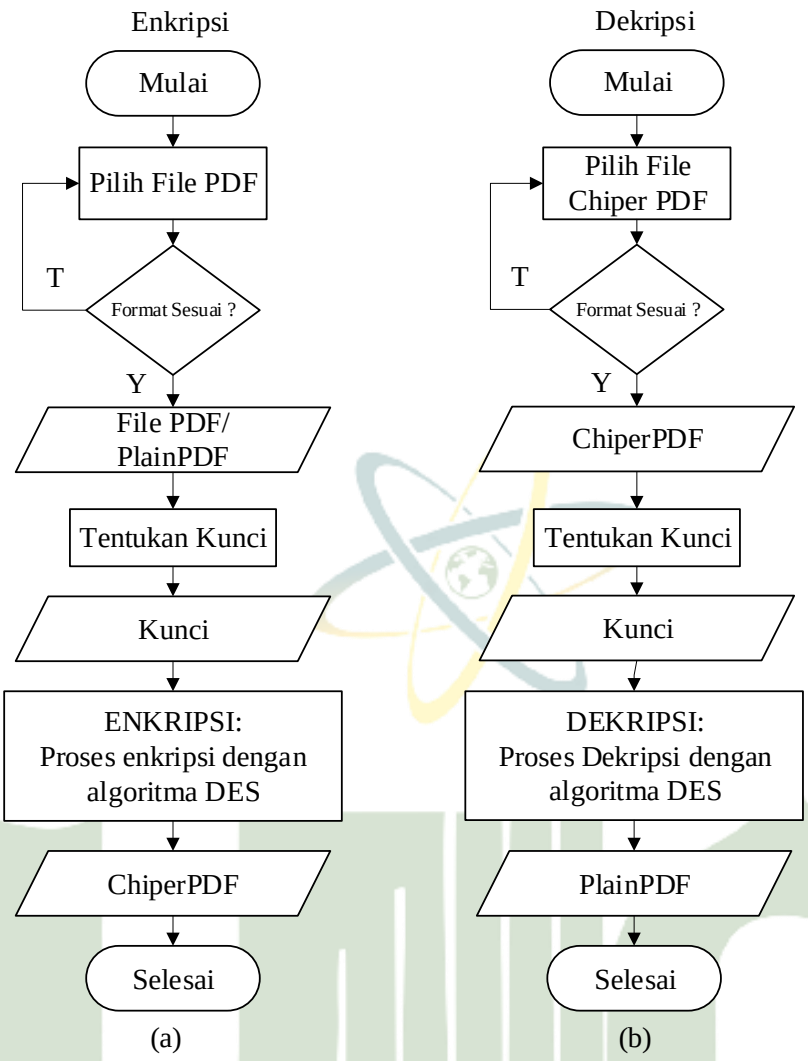
Proses dekripsi DES sama dengan proses enkripsi yaitu dilakukan sebanyak 16 ronde. Tahap pertama dilakukan dengan proses *initial permutation*, kemudian proses ronde 1 hingga ronde 16, hasil ronde 16 diproses kembali dengan teknik *final permutation*, sehingga menghasilkan *plainpdf*. Diagram dekripsi algoritma DES pada *chiperpdf* sebagai berikut:



Gambar 3.3 Diagram DekripsiDES

3.3.4Implementasi

Implementasi adalah tahapan dalam melakukan penerapan. Adapun tahapan penerapan pada penelitian ini memiliputi dari *flowchart*algoritma DES.Berikut adalah *flowchart* penerapan enkripsi dan dekripsi file dokumen PDF:



Gambar 3.4 (a)Flowchart Proses Enkripsi, dan (b) Dekripsi File PDF

3.3.5Pengujian

Pengujian sistem membahas mengenai hasil uji coba sistem yang telah di rancang. Pengujian bermaksud untuk mengetahui apakah sistem yang dibuat dapat berjalan dengan baik dan sudah memenuhi kriteria yang sesuai dengan tujuan perancangan sistem tersebut.

3.3.6 Penggunaan

Penggunaan sistem ini adalah menjelaskan sistem yang dibangun dengan menggunakan algoritma DES untuk melakukan proses pengaman file dokumen PDF berdasarkan teknik enkripsi dan dekripsi.