BAB III

METODOLOGI PENELITIAN

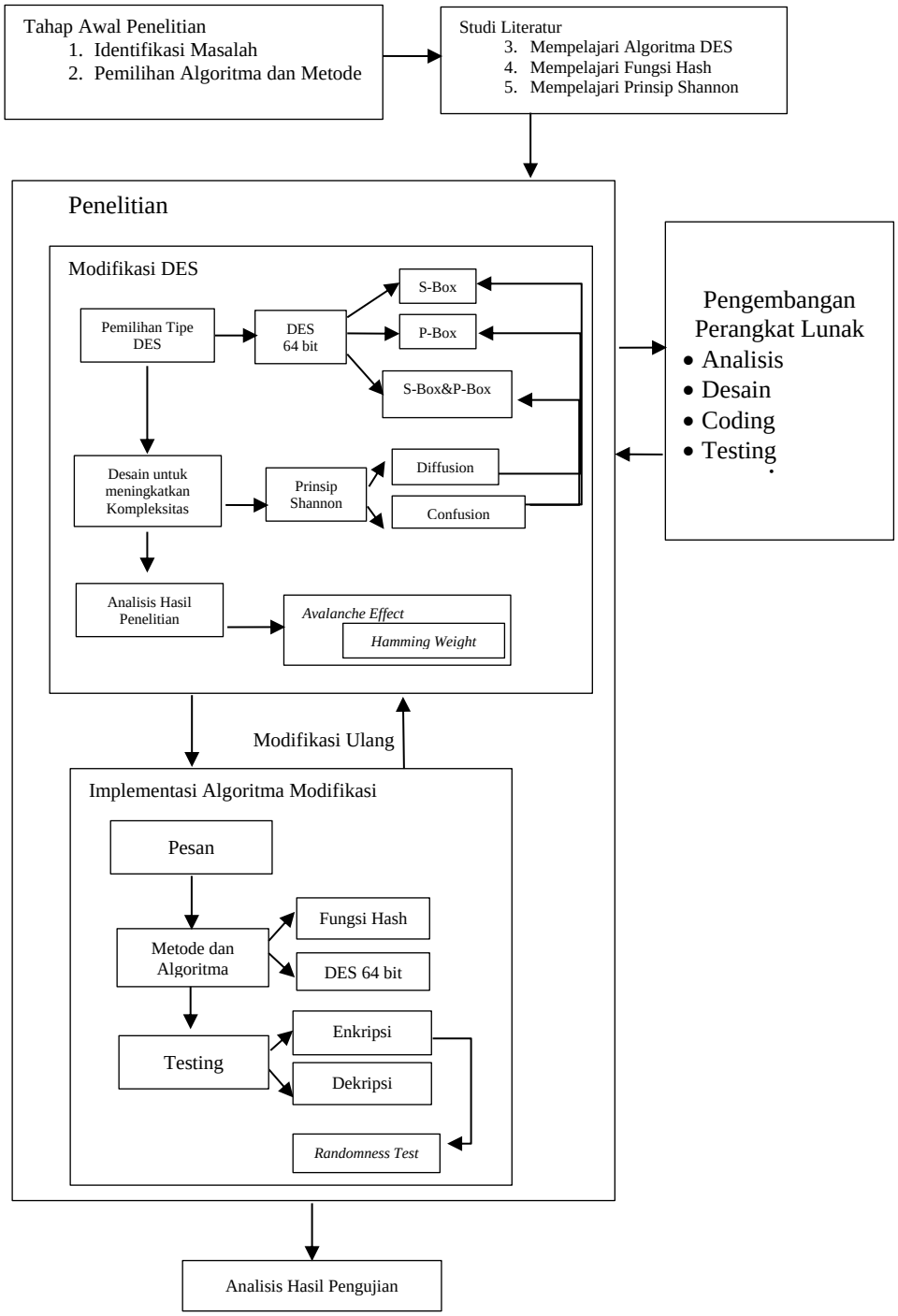
3.1 Desain Penelitian

Desain penelitian adalah tahapan atau gambaran yang akan dilakukan dalam penelitian untuk mempermudah penelitian. Desain penelitian "Modifikasi Algoritma Data Encryption Standarad (DES) 64 Bit Untuk Pengamanan Pada Penyimpanan File" dibuat untuk memberikan gambaran serta kemudahan dalam melakukan penelitian yang digambarkan seperti gambar 3.1.

Berikut ini persiapan yang dilakukan sebelum penulis mulai melakukan penelitian.

1. Menentukan kebutuhan data yang digunakan, seperti *file* yang digunakan untuk enkripsi-dekripsi, algoritma DES 64 bit, perhitungan *avalanche effect*, pengujian dengan *randomness test.*
2. Mengumpulkan data yang dibutuhkan, data yang sudah ditentukan diatas kemudian dikumpulkan untuk diproses. Data dapat diperoleh melalui studi literatur.
3. Mempersiapkan alat dan bahan penelitian. Alat disini adalah perangkat keras *(hardware)* dan perangkat lunak *(software)* yang akan digunakan memodifikasi algoritma DES 64 bit dengan pengujian *randomness test* dan *avalanche effect*, sedangkan datanya berupa data-data yang telah dikumpulkan untuk diproses ke dalam program.

   Gambaran umum mengenai desain penelitian yang penulis lakukan dapat dilihat pada gambar 3.1.



Gambar 3. 1 Desain Penelitian

Tahapan penelitian yang akan dilakukan meliputi langkah – langkah berikut :

1. Identifikasi masalah merupakan tahapan awal dalam penelitian yang dapat membantu penentuan tujuan penelitian dilakukan, masalah ditemukan dengan mengikuti isu-isu dan perkembangan teknologi saat ini, serta mempelajari penelitian yang sudah dilakukan dan dipublikasikan melaui jurnal ilmiah. Masalah yang ditemukan pada identifikasi masalah ialah ditemukannya celah untuk mengambil data pada sistem penyimpanan file dan dengan mudah membacanya serta ditemukannya celah untuk membongkar DES 64 bit.
2 Studi literatur merupakan tahapan mempelajari metode-metode yang akan digunakan pada penelitian, yaitu mempelajari proses enkripsi-dekripsi, mempelajari fungsi hash, mempelajari algoritma DES 64 bit, mempelajari prinsip Shannon untuk meningkatkan kompleksitas *Confusion* dan *Diffusion*, dan pengujian keacakan dengan *randomness test* dan *avalanche effect* baik melalui buku literatur atau jurnal ilmiah.
3 Melakukan Penelitian untuk mengenkripsi *file* yang diunggah dan mendekripsi file yang diunduh dengan memanfaatkan ilmu kriptografi.

   Penelitian yang pertama dilakukan adalah melihat hasil algoritma DES 64 bit standar dengan bantuan aplikasi cryptool 1.4.30 untuk mengetahui *randomness test* dengan beberapa kondisi kunci yang berbeda, kemudian langkah selanjutnya membuat aplikasi untuk mengetahui *avalanche effect*nya dengan matlab R2013a. setelah diketahui hasil pengujiannya. Kemudian dilakukan penelitian untuk memodifikasi DES 64 bit, dimana modifikasi terjadi untuk meningkatkan kompleksitas dari DES 64 bit standar dengan meningkatkan nilai *confusion* dan *diffusion* sesuai dengan Prinsip Shannon pada bagian *S-Box* dan *P-Box* dari algoritma DES 64 bit. DES 64-bit yang telah dimodifikasi akan dianalisis melalui beberapa tes seperti *randomness test* dengan menggunakan aplikasi cryptool 1.4.30 dan *avalanche effect* yang didalamnya terdapat *hamming weight* dengan aplikasi yang dibuat di matlab R2013a.

Tahap penelitian selanjutnya yaitu menguji algoritma DES 64 bit yang telah dimodifikasi dengan masukkan file berupa *.doc dan *.docx serta kunci yang dibangkitkan menggunakan salah satu fungsi hash yaitu sha-256 di *software package* xampp.

Selanjutnya dilakukan analisis dari hasil penelitian ini yaitu *randomness test* dengan menggunakan aplikasi cryptool 1.4.30, *avalanche effect* yang didalamnya terdapat *hamming weight* dengan aplikasi yang dibuat di matlab R2013a, ukuran *file* setelah dienkripsi apakah membesar atau mengecil serta melihat hasil dekripsinya apakah sesuai dengan file semula atau berubah. Jika ukuran file enkripsi membesar lebih dari 36% dari ukuran semula dan hasil dekripsi tidak sesuai dengan file asli maka akan kembali ke tahapan penelitian modifikasi algoritma DES 64 bit.

4 Pengembangan perangkat lunak yang mengimplementasikan hasil penelitian untuk pengujian terbatas dengan metode *waterfall*, yang terdiri dari Analisis, Desain, *Coding, Testing,* dan *Maintenance*.

3.2 Fokus Penelitian

Fokus penelitian pada skripsi ini adalah:

1. Memodifikasi bagian *S-Box* dan *P-Box* DES 64 bit.
2. Pengujian modifikasi algoritma dengan *avalanche effect* dan *randomness test*.
3. Contoh file yang bisa diolah pada modifkasi algoritma DES 64 bit ini adalah *.doc dan *.docx.
4. Tahapan-tahapan yang perlu dilakukan dalam melakukan identifikasi bagian pada DES 64 bit yang bisa diubah menjadi dinamis.

3.3 Metode Penelitian

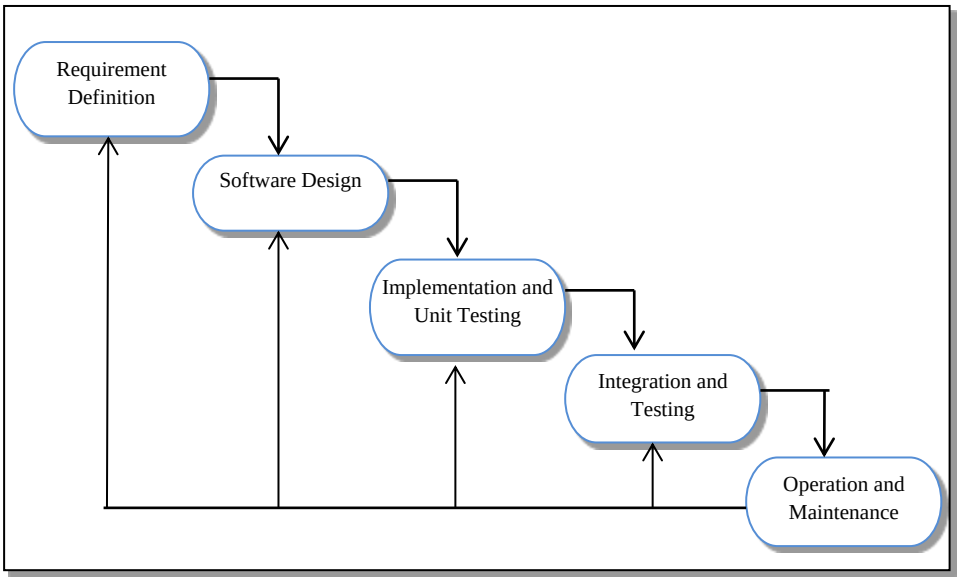
Metode penelitian ini dibagi menjadi dua, yaitu metode pengumpulan data dan metode pengembangan perangkat lunak.

3.3.1 Metode Pengumpulan Data

Dalam penelitian kali ini, data dan informasi yang tersedia dapat menunjang proses penelitian. Pada proses ini dilakukan studi literatur dengan mempelajari *fungsi hash*, algoritma DES 64 bit, struktur DES 64 bit, modifikasi DES 64 bit, *Avalanche Effect*, *Hamming Weight* dan *Randomness Test* melalui jurnal, textbook, tutorial serta dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web.*

3.3.2 Metode Pengembangan Perangkat Lunak

Pembangunan perangkat lunak dalam penilitian ini menggunakan model *waterfall* (Sommerville, 2011). Dalam model *waterfall* Sommerville terdapat kemungkinan untuk kembali ke tahap sebelumnya apabila terjadi kesalahan atau perbaikan, dimana alur prosesnya seperti pada Gambar 3.2.



Gambar 3. 2 Model *Waterfall* (Sommerville, 2011)

Berikut beberapa tahapan dari metode *waterfall* sommerville :

1. *Requirement Definition*, Tahap awal dimana adanya analisis untuk menentukan kebutuhan, batasan, dan tujuan (*goal*) dari perangkat lunak sesuai yang diinginkan. Hal tersebut kemudian didefinisikan secara rinci dan terbentuk sebagai spesifikasi sistem. Pada tahap ini dilakukan penentuan algoritma apa yang digunakan pada proses membangkitkan kode otentikasi.
2. *Software Design* merupakan proses perancangan yang melibatkan identifikasi dan menggambarkan dasar sistem serta hubungan satu sama lain. Pada tahap ini dibuat desain dari implementasi algoritma yang akan dikembangkan yaitu proses otentikasi pengguna baru.
3. *Implementation and Unit Testing*, Pada tahap ini, *software design* yang telah dilakukan sebelumnya kemudian diimplementasikan dalam bentuk unit program. Setelah unit program dibuat, kemudian

dilakukan *testing* pada unit program tersebut untuk memastikan implementasi berjalan dengan baik.

4. *Integration and Testing,* Setelah semua unit program berhasil diimplementasikan dan lolos *testing* maka dilanjutkan dengan mengintegrasikan setiap unit untuk membentuk aplikasi yang diinginkan. Aplikasi yang sudah dibentuk kemudian di tes kembali untuk memastikan unit program dapat berjalan satu sama lain dalam aplikasi dan aplikasi yang dibuat sudah memenuhi kebutuhan.
5. *Operation and Maintenance*, Tahap ini merupakan tahap dimana aplikasi sudah dipasang kemudian melakukan perbaikan ketika terdapat kesalahan atau *error* yang tidak ditemukan sebelumnya saat pembangunan aplikasi berlangsung. Perbaikan juga dilakukan jika terdapat kebutuhan baru yang perlu ada pada aplikasi.

3.4 Alat dan Bahan Penelitian

Berdasarkan kebutuhan-kebutuhan di atas, maka ditentukan bahwa alat dan bahan yang digunakan pada penelitian ini adalah sebagai berikut:

3.4.1 Alat Penelitian

Dalam penelitian ini, peneliti menggunakan bebagai alat bantu penunjang baik berupa perangkat keras maupun perangkat lunak. Adapun perangkat keras yang digunakan adalah seperangkat komputer yang mempunyai spesifikasi sebagai berikut:

1. *Processor* Intel i7
2. RAM 4 GB
3. *Hard disk* 1000 GB
4. Mouse dan Keyboard

Sementara itu perangkat lunak yang digunakan adalah sebagai berikut:

1. Sistem Operasi Microsoft Windows 8.1 64 bit
2. Notepad++
3. Xampp
4. MySQL
5. Chrome
6. Matlab R2013a
7. Cryptool 1.4.30

3.4.2 Bahan Penelitian

Bahan penelitian yang digunakan adalah jurnal penelitian yang sudah dilakukan, *textbook*, *tutorial*, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang *fungsi hash*, algoritma DES, *Avalanche Effect, Randomness Test.*

3.4.3 Bahan Pengujian Algoritma

Beberapa bahan yang digunakan untuk pengujian algoritma yaitu Kunci masukkan, perhitungan nilai kunci dengan *xor*, perubahan alur untuk modifikasi *S-Box* dan *P-Box.*

3.4.3.1 Kunci Masukkan

Kunci masukkan yang digunakan pada penelitian ini yaitu

Tabel 3. 1 Kunci Masukkan

No	Kunci

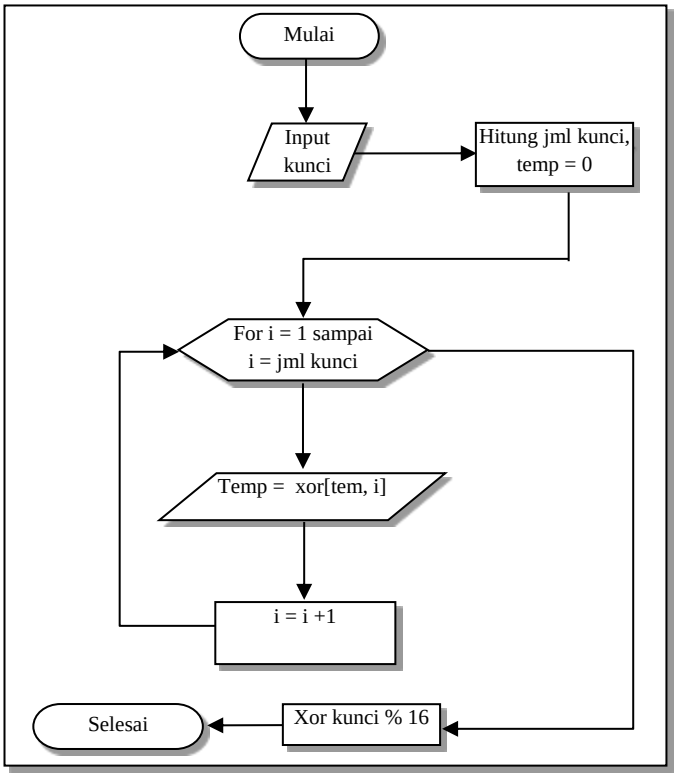
1	00000000
2	01010101
3	10101010
4	11111111
5	Alfabet
6	Alfanumerik

Beberapa dari kunci pada tabel 3.1 merupakan kunci lemah untuk algoritma DES.

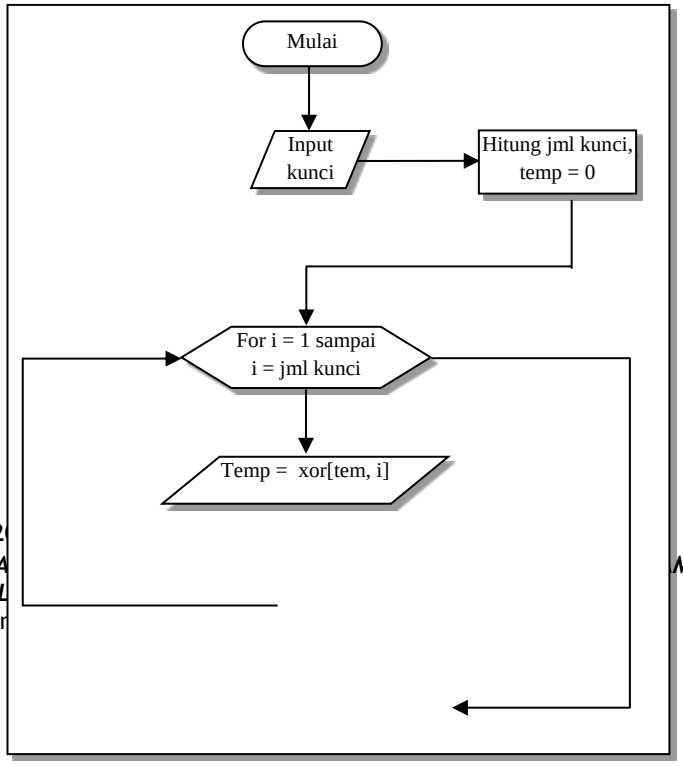
3.4.3.2 Perhitungan Nilai Kunci Dengan *Xor*

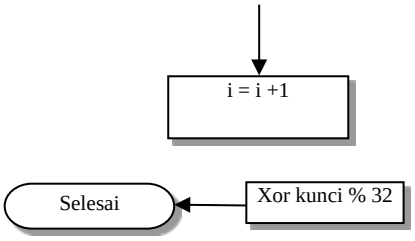
Nilai *xor* kunci yang digunakan untuk membuat nilai tabel *S-Box* dan *P-Box* menjadi dinamis, berikut langkah-langkah yang digunakan untuk mendapatkan nilai *xor* kunci :

1. Hitung jumlah karakter kunci.
2. Buat perulangan dengan batas jumlah karakter kunci.
3. Ubah ke dalam biner perkaraker dari kunci.
4. *Xor*-kan nilai biner dari karakter sebelumnya dengan nilai biner dari karakter selanjutnya.
5. Setelah selesai perulangan, ambil nilai *xor* kunci.
6. Untuk *S-Box* di mod 16 dan untuk *P-Box* di mod 32, sesuai nilai *max* pada masing-masing tabel.



Gambar 3. 3 Gambar Alur *Xor* Kunci *S-Box*





Gambar 3. 4 Gambar Alur *Xor* Kunci *P-Box*

3.4.3.3 Perubahan Alur Untuk Modifikasi *S-Box* Dan *P-Box*

Perubahan yang dilakukan pada modifikasi *S-Box* yaitu merubah nilai pada tabel *S-Box* yang bisa dilihat pada gambar 2.8 agar lebih dinamis dan tergantung pada kunci masukkan, pada penelitian ini nilai dari tabel *S-Box* di-*xor* dengan hasil *xor* kunci sehingga nilai tabel *S-Box* setiap kali memproses tidak akan sama, hal ini berlaku juga pada tabel *P-Box* dimana nilai tabel *P-Box* dari hasil modifikasi ini akan lebih dinamis.

3.4.4 Bahan Pengujian Implementasi Algoritma

Beberapa bahan yang digunakan untuk pengujian implementasi algoritma yaitu jenis file, karakteristik file, hasil enkripsi-dekripsi.

3.4.4.1 Jenis *File*

Contoh Jenis *file* yang digunakan pada penelitian ini adalah *file* dokumen berekstensi *.doc dan *.docx dengan bebrapa ukuran dan konten *file* yang berbeda-beda.

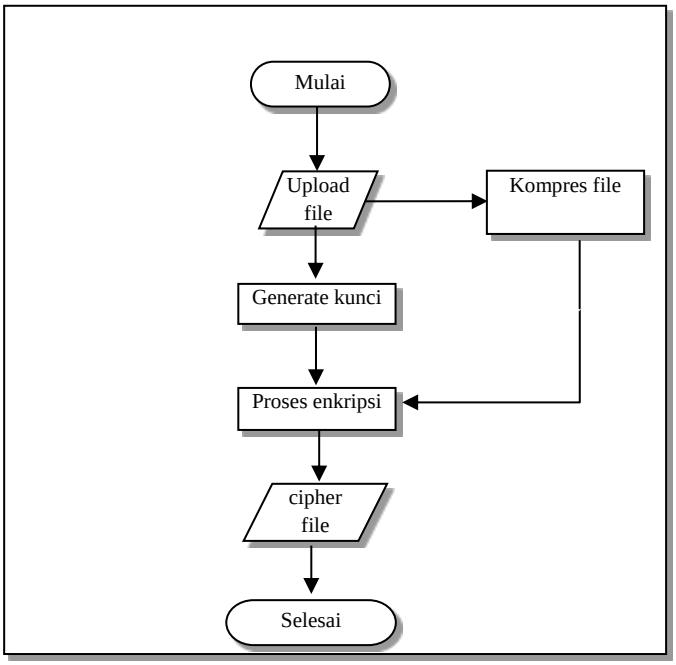
Tabel 3. 2 Ukuran *File* Dokumen

No	Ukuran *file*
1	351KB
2	2868KB

3	6655KB

3.4.4.2 Implementasi Enkripsi DES 64 Bit

Pada penelitian implementasi algoritma ini digunakan 2 proses yang berbeda, yaitu implementasi algoritma DES 64 bit dengan fungsi kompresi dan implementasi algoritma DES 64 bit saja yang akan berpengaruh pada ukuran *file* hasil enkripsi. Pada penelitian implementasi yang pertama yaitu dengan menggunakan algoritma DES 64 bit dan fungsi kompresi *file* yang digunakan sehingga *file* yang akan dienkripsi ukurannya lebih kecil. Alur proses enkripsi dengan kompresi seperti pada gambar 3.5.



Gambar 3. 5 Gambar Alur Enkripsi DES 64 bit dengan Fungsi Kompresi

Pada penelitian implementasi yang kedua yaitu dengan menggunakan algoritma DES 64 bit saja yang digunakan. Alur proses enkripsi tanpa kompresi seperti pada gambar 3.6.