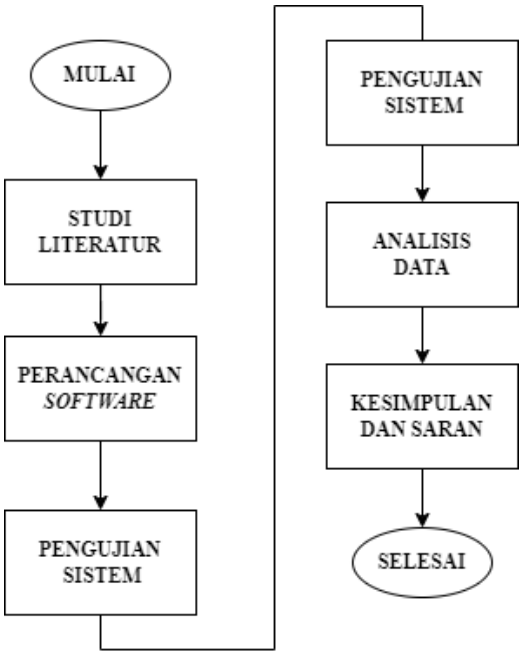
# BAB III
# METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini meliputi dua aspek, yaitu metode pengumpulan data dan metode pengembangan sistem. Dalam pengumpulan data, penelitian ini menggunakan metode untuk mempelajari dan mengumpulkan literatur yang terkait dengan penerapan algoritma kriptografi *twofish* dalam proses enkripsi dan dekripsi. Dalam penelitian ini juga akan melakukan studi terhadap penelitian sebelumnya yang terkait dengan enkripsi dan dekripsi. Sumber data yang digunakan meliputi jurnal ilmiah, makalah, artikel dan sumber ilmiah lainnya. Berikut adalah tahapan-tahapan penelitian yang dilakukan:

## 3.1 ALUR PENELITIAN

Pada penelitian ini, ada beberapa yang akan dilakukan untuk mewujudkan hasil yang diharapkan. Berikut ini merupakan tahapan pelaksanaan perancangan algoritma kriptografi *twofish* untuk menyembunyikan data berupa pesan teks yang akan dijelaskan melalui blok diagram sebagaimana ditunjukkan pada gambar 3.1.




**Gambar 3.1 Blok diagram penelitian**

Gambar 3.1 merupakan diagram mengenai tahapan alur penelitian. Tahapan alur penelitian tersebut meliputi studi literatur, perancangan *software*, pengujian sistem, pengambilan data, analisis data, serta yang terakhir adalah kesimpulan dan

saran. Penjelasan untuk tahapan penelitian dari diagram alur di atas adalah sebagai berikut:

1. Studi literatur

   Pada tahap studi literatur bertujuan untuk mengumpulkan mempelajari dan mengolah bahan penelitian mengenai algoritma kriptografi *twofish*, serta *software* yang digunakan untuk mendukung penelitian serta alat dan bahan yang perlu dikumpulkan pada saat melakukan analisis mengenai algoritma *twofish*. Untuk sumber referensi yang digunakan sebagian besar didapatkan dari jurnal dan artikel. Terdapat beberapa juga yang diambil dari *website* yang terpercaya (bukan diambil dari blogspot atau wordpress).

2. Perancangan *software*

   Tahapan kedua yang dilakukan yaitu perancangan *software*. Pada tahap ini akan disusun program yang akan mendukung berjalannya penelitian ini, perancangan *software* ini meliputi pembuatan program sederhana menggunakan Python yang akan memakai komputer berbasis Windows.

3. Pengujian system

   Setelah perancangan *software* sudah dilakukan, maka langkah selanjutnya adalah pengujian sistem. Pada tahap ini, pengujian dilakukan untuk mengetahui apakah *software* yang telah dirancang sudah sesuai dengan hasil yang diharapkan atau tidak. Pengujian yang dilakukan tentunya adalah algoritma *twofish* dalam mengenkripsi dan dekripsi suatu data berupa pesan teks sudah dapat dilakukan atau belum. Apabila hasilnya sudah dirasa sesuai dan cukup, maka dapat dilakukan tahapan selanjutnya yaitu pengambilan data dari hasil pengujian system.

4. Pengambilan data

   Setelah pengujian sistem, terdapat sebuah hasil berupa kecepatan enkripsi dan dekripsi, kunci keamanan hasil enkripsi dan dekripsi; dan sebagainya. Hasil yang didapatkan tersebut akan dikumpulkan untuk dapat dianalisis ke tahapan selanjutnya. Sehingga, setelah data berhasil

didapatkan, maka hal yang akan dilakukan selanjutnya adalah analisis data.

5. Analisis data

   Data yang sudah diperoleh pada tahap pengumpulan data, akan diolah dan dianalisis pada tahapan ini, data tersebut dianalisis sehingga dapat diketahui alasan dari perolehan parameter yang didapatkan Ketika pengujian dilakukan.

6. Kesimpulan dan saran

   Tahapan yang terakhir adalah penyusunan kesimpulan dan saran terkait hasil penelitian yang sudah dilaksanakan.

## 3.2 ALAT DAN BAHAN

### 3.2.1 PERANGKAT KERAS (*HARDWARE*)

Perangkat keras atau *hardware* yang digunakan pada penelitian kali ini hanya menggunakan satu perangkat laptop dengan spesifikasi seperti terlihat pada tabel 3.1.

**Tabel 3.1 Penggunaan perangkat keras dan fungsinya**

| | |
|---|---|
| **Sistem Operasi** | Windows 11 Pro |
| **Prosesor** | Intel Core i5-3230M CPU @ 2.60GHz (4 CPUs) |
| **RAM** | 8 GB |
| **ROM** | 256 GB |

### 3.2.2 PERANGKAT LUNAK (*SOFTWARE*)

Pada penelitian kali ini bertujuan untuk menganalisa kinerja algoritma kriptografi *twofish* dengan melakukan enkripsi dan dekripsi terhadap pesan teks dan *file* gambar yang diimplementasikan melalui sebuah *website localhost* pengiriman pesan teks dan *file* gambar. Berikut rincian *software* aplikasi yang digunakan:

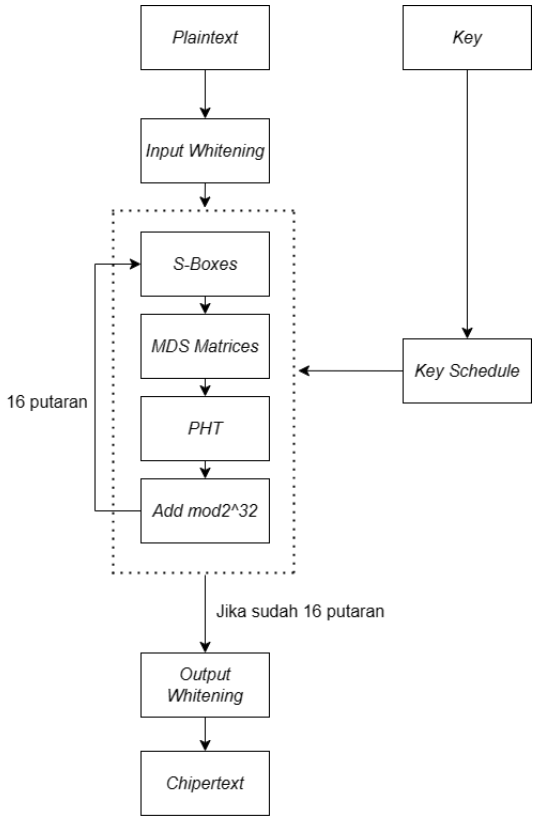
**Tabel 3.2 Penggunaan perangkat lunak dan fungsinya**

| No | Nama Software | Versi | Fungsi |
|---|---|---|---|
| 1 | Visual Studio Code | v1.61.2 | Untuk merancang kriptografi *twofish* dan merancang desain *website* localhost |

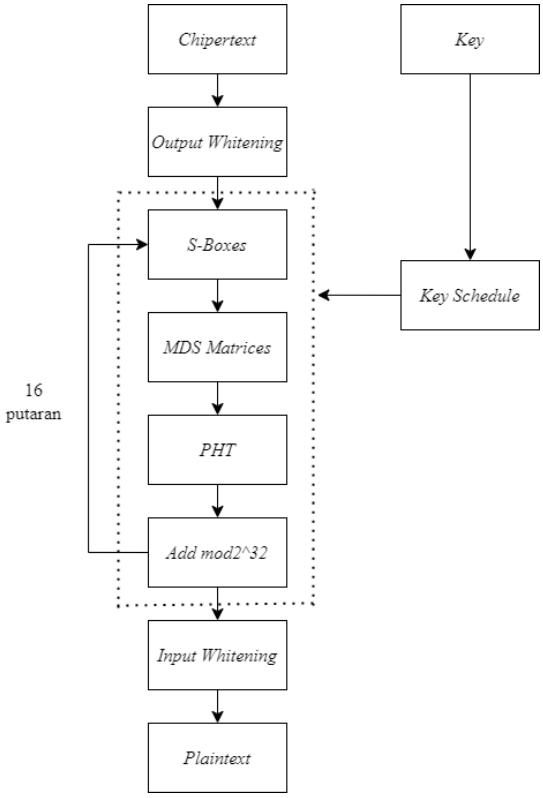
| No | Nama Software | Versi | Fungsi |
|---|---|---|---|
| 2 | Ms Edge | v114.0.1823.67 | Untuk pengujian hasil enkripsi dan dekripsi dan pengujian *website localhost* sudah berjalan atau belum |

## 3.3 BLOK DIAGRAM SISTEM KERJA *TWOFISH*

Penelitian ini memanfaatkan algoritma kriptografi *twofish* untuk menyembunyikan sebuah data, yang fungsi utamanya adalah agar data tersebut tidak mudah diketahui oleh pihak yang tidak berwenang. Pada penelitian ini juga terdapat sebuah blok diagram dari sistem kerja dari pemanfaatan algoritma kriptografi *twofish.* Pada blok diagram gambar 3.2 tertampil sistem blok diagram enkripsi untuk pengiriman pesan teks dan gambar dan untuk blog diagram gambar 3.3 tertampil sistem blok dekripsi untuk pembacaan kembali atau menampilkan pesan teks dan gambar yang sesuai dengan hasil enkripsi sebelumnya.




**Gambar 3.2 Blok diagram cara kerja enkripsi algoritma *twofish***




**Gambar 3.3 Blok diagram cara kerja dekripsi algoritma *twofish***

Gambar 3.2 adalah ilustrasi dari blok diagram cara kerja enkripsi data menggunakan algoritma *twofish*, pada blok diagram perlu dua masukan, yaitu *plaintext* atau teks yang hendak dienkripsi dan juga *key* atau kunci yang diperlukan untuk proses enkripsi. Kemudian, kunci atau *key* tersebut akan masuk proses penjadwalan kunci, yang nantinya akan dimasukkan pada proses *whitening plaintext*. Pada proses *whitening*, akan mengalami beberapa langkah hingga dari langkah tersebut diulang hingga 16 putaran, karena *twofish* menerapkan sebuah sistem jaringan Feistel yang terdiri dari 16 putaran. Proses *whitening* ini melibatkan operasi XOR pada kunci sebelum putaran pertama dan setelah putaran terakhir. Selain elemen-elemen standar yang ada dalam jaringan Feistel, algoritma *twofish* juga mencakup teknik pemutihan dan kunci pengganti yang dikenal sebagai *whitening key*. Setelah tahap *whitening* selesai, maka *output* dari hasil tersebut akan keluar berupa *chipertext*. Ketika sebuah *plaintext* berubah menjadi *chipertext*, berarti telah berhasil dilakukan proses enkripsi.

Gambar 3.3 adalah ilustrasi dari blok diagram cara kerja dekripsi data menggunakan algoritma *twofish*, pada dasarnya serupa dengan enkripsi data, hanya saja alur yang dibalik dengan memasukan *chipertext* yang hendak didekripsi dan

juga kunci yang dipakai pada saat enkripsi untuk hasil yang sesuai, karena jika kunci yang digunakan berbeda, maka hasil yang didapatkan akan salah. Setelah itu, akan dimasukan ke proses *output whitening* berupa *swap* blok dan diputar kembali sebanyak 16 kali melewati tahapan *S-boxes, MDS Matrices, PHT,* dan penambahan modulasi. Jika semua sudah selesai diputar hingga 16 kali, maka akan kembali lagi ke *input whitening* yang nantinya akan menghasilkan *plaintext* seperti pada saat sebelum enkripsi.

## 3.4 *FLOWCHART* SKENARIO PENGUJIAN

Penelitian ini menggunakan algoritma kriptografi *twofish* untuk mengenkripsi dan dekripsi pesan teks (biasa seperti SMS) dan *file* gambar (jpg. atau png.). Alur system kerja pengiriman dapat dilihat pada *flowchart* di gambar 3.4.


**Gambar 3.4 Alur system kerja penggunaan *twofish* pada penelitian ini**

Algoritma *twofish* tersebut akan digunakan untuk mengenkripsi dan dekripsi file teks biasa dan file gambar dengan format jpg. atau png. kemudian, pada bagian enkripsi dan dekripsi tersebut, akan terdapat beberapa parameter yang akan diujikan, yaitu hasil enkripsi maupun dekripsi, dan juga waktu enkripsi maupun dekripsi terhadap pesan teks dan file gambar dengan ukuran yang berbeda-beda.

Dalam penelitian ini, akan dilakukan pengujian terhadap pesan teks dengan panjang karakter yang berbeda-beda dan juga file gambar berformat jpg. atau png. dengan ukuran berbeda-beda. Seperti terlihat pada tabel 3.3 dan tabel 3.4.

**Tabel 3.3 Jumlah karakter pesan teks uji sistem**

| No | Jenis File | Panjang Karakter | Teks yang dienkripsi |
|---|---|---|---|
| 1 | Pesan teks biasa | 20 | Aku adalah mahasiswi |
| 2 | Pesan teks biasa | 40 | Aku adalah mahasiswi ITTelkom Purwokerto |
| 3 | Pesan teks biasa | 70 | Aku adalah mahasiswi ITTelkom Purwokerto yang berasal dari Jawa Tengah |
| 4 | Pesan teks biasa | 105 | Aku adalah mahasiswi ITTelkom Purwokerto yang berasal dari Jawa Tengah dengan Prodi Teknik Telekomunikasi |

| No | Jenis File | Panjang Karakter | Teks yang dienkripsi |
|---|---|---|---|
| 5 | Pesan teks biasa | 200 | Aku adalah mahasiswi ITTelkom Purwokerto yang berasal dari Jawa Tengah dengan Prodi Teknik Telekomunikasi yang mempelajari algoritma kriptografi *twofish* untuk dijadikan skripsi |

**Tabel 3.4 Jumlah ukuran gambar uji sistem**

| No | Nama File | Jenis File | Ukuran (*bytes*) |
|---|---|---|---|
| 1 | Gambar 1 | JPG/PNG | 8.811 |
| 2 | Gambar 2 | JPG/PNG | 103.375 |
| 3 | Gambar 3 | JPG/PNG | 1.096.885 |
| 4 | Gambar 4 | JPG/PNG | 2.450.558 |
| 5 | Gambar 5 | JPG/PNG | 6.268.405 |

Berikut untuk sampel gambar yang akan digunakan pada pengujian kali ini yang berjumlah 5 sampel.


**Gambar 3.5 Sampel percobaan pertama [22]**

**Gambar 3.6 Sampel percobaan kedua [23]**

**Gambar 3.7 Sampel percobaan ketiga [23]**

**Gambar 3.8 Sampel percobaan keempat [23]**

**Gambar 3.9 Sampel percobaan kelima [23]**

Setelah itu, ketika semua pengujian sudah dilakukan, langkah selanjutnya adalah dengan menganalisis terhadap data-data yang sudah didapatkan untuk mengetahui seberapa efektif dalam menggunakan kriptografi *twofish* dalam mengenkripsi dan dekripsi sebuah pesan teks maupun *file* gambar.