BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian yang dilakukan merupakan penelitian eksperimental, yaitu penelitian yang pengumpulan datanya melalui pencatatan secara langsung dari hasil percobaan yang dilakukan.

3.2 Instrumen Penelitian

Dalam penelitian ini, dibutuhkan beberapa instrumentasi peralatan, diantaranya :

3.2.1 Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak merupakan faktor yang harus dipenuhi dalam penelitian ini, sehingga perangkat lunak tersebut sesuai dengan maksud dan tujuan dalam penelitian.

Perangkat lunak yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

a. Sistem Operasi

   Sistem operasi yang dapat digunakan dalam penelitian ini adalah Windows 7 64-bit. Alasan menggunakan sistem operasi ini adalah karena sebagian besar masyarakat cukup familiar dalam penggunaannya.

b. Visual Basic 6.0

   Software ini digunakan sebagai *tool* untuk melakukan proses dalam penelitian. Visual Basic 6.0 memudahkan dalam implementasi selain itu juga dapat membuat form yang relatif mudah dan lebih menarik.

c. Microsoft Office Word 2007

Software ini digunakan untuk menyusun laporan hasil dari penelitian. Proses penulisan menggunakan Microsoft Office Word, karena software tersebut sudah dikenal dan digunakan secara luas. Microsoft Office Word merupakan pengolah data yang dianjurkan sebagai spesifikasi minimal, karena ekstensi yang sering digunakan adalah format .docx dan .doc yang dapat dijalankan pada software ini.

3.2.2 Kebutuhan Perangkat Keras

Perangkat keras juga dibutuhkan pada penelitian ini. Perangkat keras yang digunakan pada penelitian ini adalah sebagai berikut :

a. Personal Computer atau laptop dengan spesifikasi :
   - Processor : AMD Athlon 64 X2 L310 @1.20 GHz
   - RAM: 2.00 GB DDR2
   - Harddisk: 320 GB 5400rpm
   - VGA : ATI Mobility Radeon HD 3200
b. Mouse
c. Printer

3.3 Prosedur Pengumpulan Data

Pada metode pengumpulan data untuk mendapatkan data yang cukup akurat, maka digunakan beberapa metode di bawah ini yaitu :

a. Studi pustaka

   Dengan metode pengambilan data secara umum, didapat data-data yang diambil dari bermacam-macam buku, literatur, dan referensi. Selain itu pengumpulan data juga diambil dari media maya yaitu internet. Sehingga data-data yang diambil dapat mendukung dan melengkapi untuk membantu dalam melakukan penelitian.

b. Eksperimen

Setelah mendapatkan data secara studi pustaka, proses penelitian akan dilakukan eksperimen atau percobaan. Dalam eksperimen ini pengumpulan data dapat diambil secara langsung, sehingga akan lebih mendalami dalam melakukan penelitian. Peneliti juga melakukan percobaan berulang-ulang untuk menghindari dan meminimalkan kesalahan dalam penelitian ini.

3.4 Teknik Analisa Data

Dalam penelitian ini, akan dilakukan beberapa teknik analisa data yang diantaranya sebagai berikut:

1. Mencari data pesan berjenis teks atau bertipe teks (.txt) yang akan dienkripsi dalam kegiatan penelitian.
2. Mengubah data-data dalam bentuk hexadesimal untuk proses enkripsi dan dekripsi.

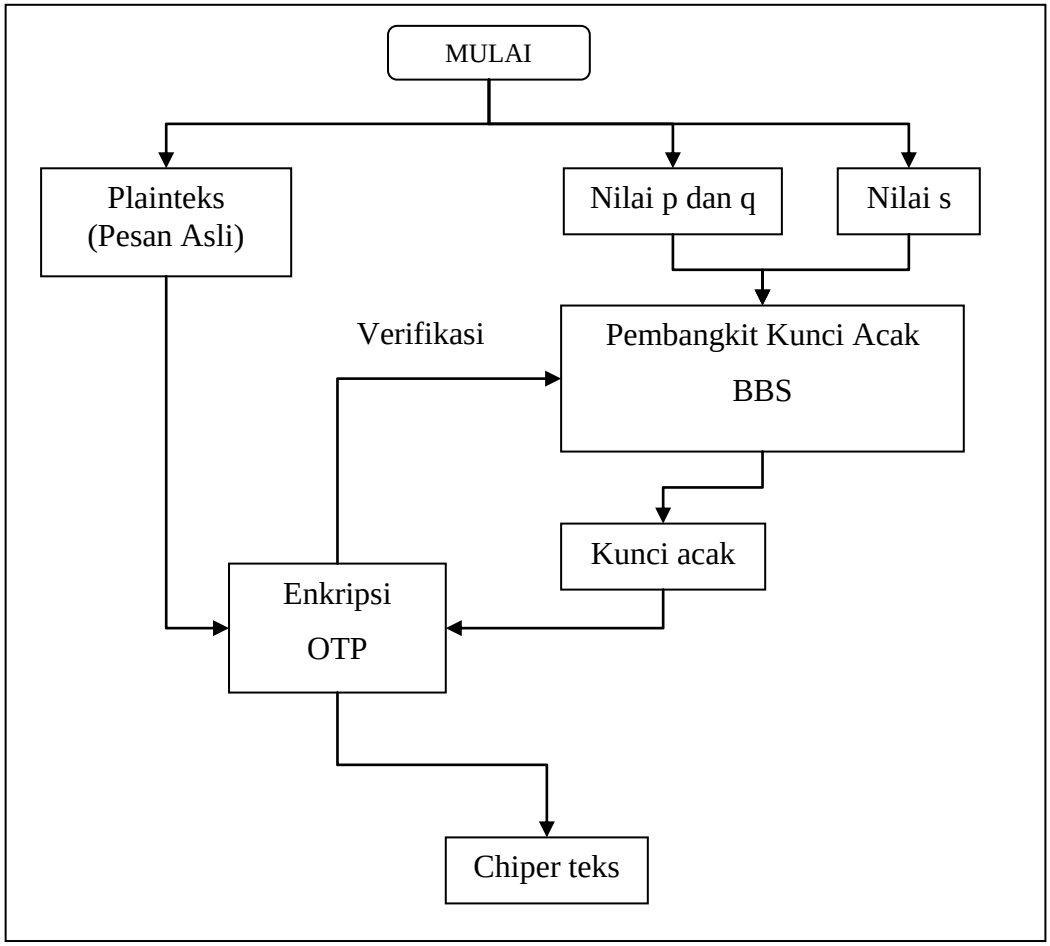
3.5 Metode yang Diusulkan

Metode yang diusulkan meliputi pembangkitan kunci acak semu *BBS* (*Blum Blum Shub*) , penerapan kunci pada algoritma *OTP* (*One Time Pad*). Pada kriptografi, ada beberapa komponen terpenting yang harus ada yaitu plainteks, kunci, dan cipherteks. Ketiga komponen tersebut adalah bahan utama untuk melakukan proses enkripsi dan dekripsi. Pada penelitian ini, komponen kunci menjadi pembahasan utama yaitu di mana algoritma BBS (Blum Blum Shub) akan diterapkan pada algoritma *OTP* (*One Time Pad*). Komponen kunci yang dihasilkan akan digunakan dalam proses enkrispsi dan dekripsi, serta kunci-kunci yang sudah dibangkitkan sebelumnya akan divariasi untuk memperbanyak kunci yang ada sebelumnya.

3.5.1 Prosedur Enkripsi Data yang Diusulkan

Pesan awal atau *Plainteks* akan dienkripsi dengan kunci acak semu menggunakan algoritma *One Time Pad* (OTP) sehingga menghasilkan *cipherteks*.

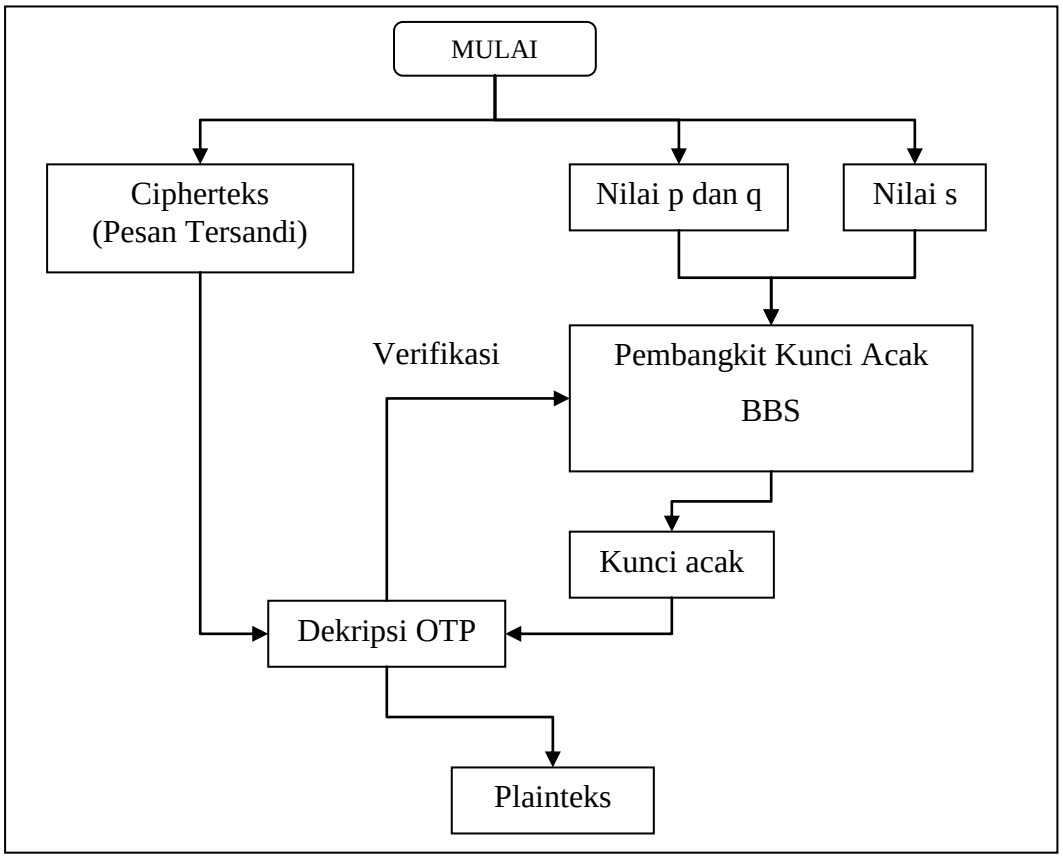
Pada proses enkripsi pada algoritma OTP diperlukan kunci sepanjang plainteks, sehingga diperlukan kolaborasi antara algoritma enkripsi dengan pembangkit kunci melalui proses verifikasi. Untuk membangkitkan kunci yang semu acak, penggunaan algoritma *BBS* (*Blum Blum Shub*) yang mempunyai properti yang berharga bagi kriptografi. Pembangkit kunci dengan *Blum Blum Shub* yaitu tergantung pada nilai *p*, *q*, dan *s* yang dimasukan, serta panjang kunci tergantung hasil dari algoritma pembangkit kunci dan plainteks. Di bawah ini adalah desain garis besar untuk proses enkripsi dalam penelitian ini :



Gambar 1 : Flowchart Metode Enkripsi

3.5.2 Prosedur Dekripsi Data yang Diusulkan

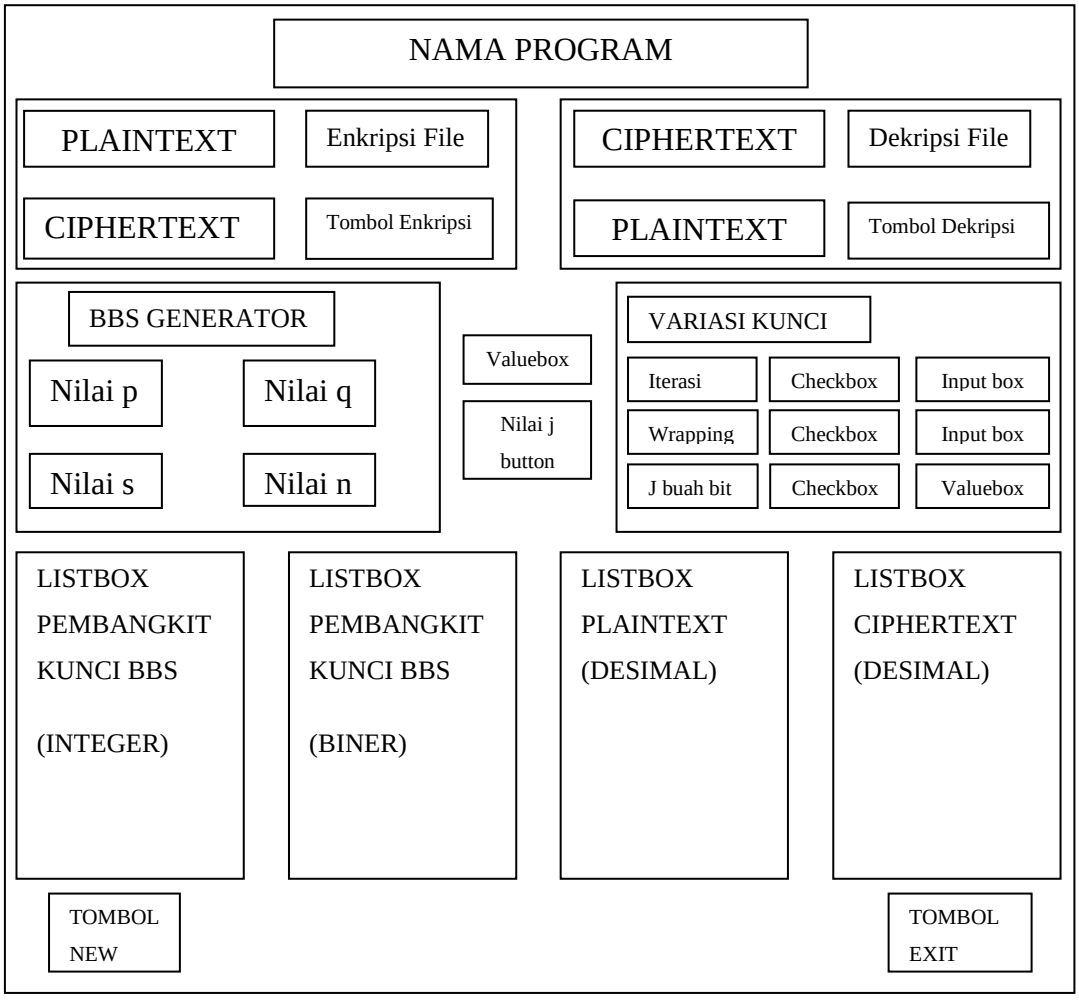
Pesan yang tersandi (*Cipherteks)* akan dekripsi dengan kunci acak semu menggunakan algopritma *One Time Pad* (OTP) sehingga menghasilkan *plainteks*. Untuk membangkitkan kunci yang semu acak, penggunaan menggunakan algoritma *BBS* (*Blum Blum Shub*) yang mempunyai properti yang berharga bagi kriptografi. Pada proses enkripsi pada algoritma OTP diperlukan kunci sepanjang plainteks, sehingga agar hasil dekripsi relevan dan valid, maka cipherteks akan dibandingkan dahulu dengan hasil nilai-nilai pembangkit kunci acak, sehingga diperlukan kolaborasi antara algoritma dekripsi dengan pembangkit kunci melalui proses verifikasi. Pembangkit kunci dengan *Blum Blum Shub* yaitu tergantung pada nilai *p*, *q*, dan *s* yang dimasukan, serta panjang kunci tergantung hasil dari algoritma pembangkit kunci dan cipherteks. Di bawah ini adalah desain garis besar untuk proses dekripsi dalam penelitian ini :



Gambar 2 : Flowchart Metode Dekripsi

3.6 Desain Tampilan Program

Dalam pembuatan pada aplikasi, terdapat desain pada program, termasuk didalamnya tampilan input dan output. Di bawah ini adalah desain tampilan pada program yang akan dibuat :



Gambar 3 : Desain Tampilan Program

Pada desain aplikasi Blum Blum Shub dan *One Time Pad* di atas ada form inputan dan keluaran yaitu form untuk dekripsi di sebelah kanan gambar dengan perintah tombol dekripsi dan form untuk enkripsi di sebelah kiri gambar dengan perintah tombol enkripsi. Dibawah form enkripsi, terdapat form BBS Generator yang merupakan pembangkit kunci bilangan semu acak pada program ini. Pada

form BBS Generator terdapat tombol Run yang berfungsi untuk menjalan kunci sebelum proses enkripsi dan dekripsi, selain itu dapat memverifikasi inputan yang dimasukan pengguna sudah sesuai dengan syarat-syarat algoritma BBS atau belum. Penempatan pemilihan iterasi dan *wrapping* yang merupakan proses variasi kunci pada *One Time Pad*, ditempatkan dibawah form dekripsi. Selain form tersebut, ada listbox yang di dalamnya berupa daftar nilai-nilai yang akan muncul setelah dilakukannya perintah menjalankan program. Listbox tersebut diharapkan untuk lebih menjelaskan bagaimana jalannya perubahan dari plainteks ke cipherteks atau sebaliknya.

3.7 Eksperimen dan Cara Pengujian Metode

Sebelum melakukan penelitian, akan dilakukan pengumpulan data terlebih dahulu. Seperti yang telah diketahui bahwa pengumpulan data diambil secara pustaka. Setelah data berhasil dikumpulkan, dilakukan percobaan pada metode kriptografi antara algoritma *One Time Pad* dengan algoritma BBS. Dalam penelitian ini akan dilakukan beberapa pengujian pada metode yang telah diusulkan, pengujian yang akan dilakukan diantaranya :

- Pengujian Fungsi Program
  Pengujian ini dilakukan dengan menguji tombol-tombol, dan fungsi-fungsi yang ada pada program.
- Tingkat Error dan Random Sampling
  Pada pengujian tingkat error ini, dilakukan sebanyak seratus kali percobaan dengan menginputkan teks yang berbeda-beda ke dalam aplikasi yang sudah dibuat. Dan dari seratus file teks tersebut sudah dilampirkan. Dalam mengukur tingkat error dimana aplikasi dapat melakukan proses enkripsi lalu mendekripsikan pesan sehingga harus menghasilkan plainteks yang sama dengan sebelumnya. Lalu akan melakukan persentase error dari sebesar 0 persen sampai 100 persen. Pengujian ini dilakukan dengan mengambil sampel acak. Sampel acak yang diambil berupa teks atau file bertipe teks (.txt).