BAB III
METODE PENELITIAN

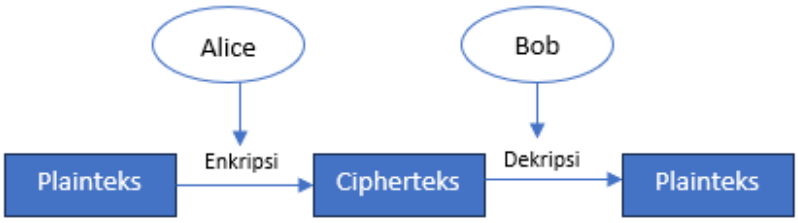
3.1 Identifikasi Masalah

Dalam penelitian ini dilakukan pengamanan terhadap pesan teks menggunakan kriptografi *hybrid*, yakni mengkombinasi antara algoritma *atbash -autokey cipher* (sebagai kriptografi simetri) dan algoritma El Gamal (sebagai kriptografi asimetri). Kriptografi pertama adalah *atbash cipher*, yang dilanjutkan *autokey cipher* dengan kunci berupa karakter, sehingga terakhir adalah algoritma El Gamal dengan memanfaatkan kunci berupa bilangan prima. Dan akhirnya akan diperoleh pesan tersamar berupa bilangan.

3.2 Model Dasar

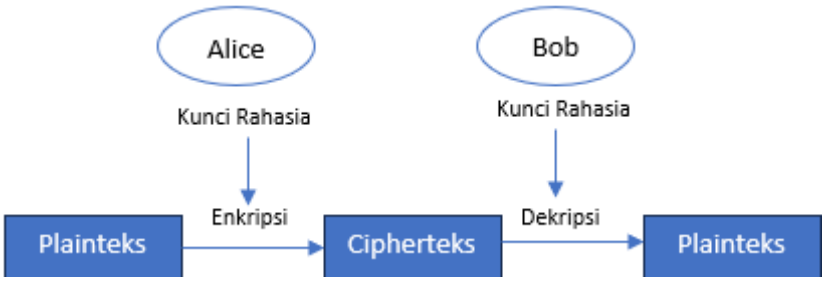
Model dasar yang dipakai di dalam penelitian ini adalah algoritma *atbash - autokey cipher* dan algoritma El Gamal.

Skema *atbash cipher* ditunjukkan pada gambar berikut:



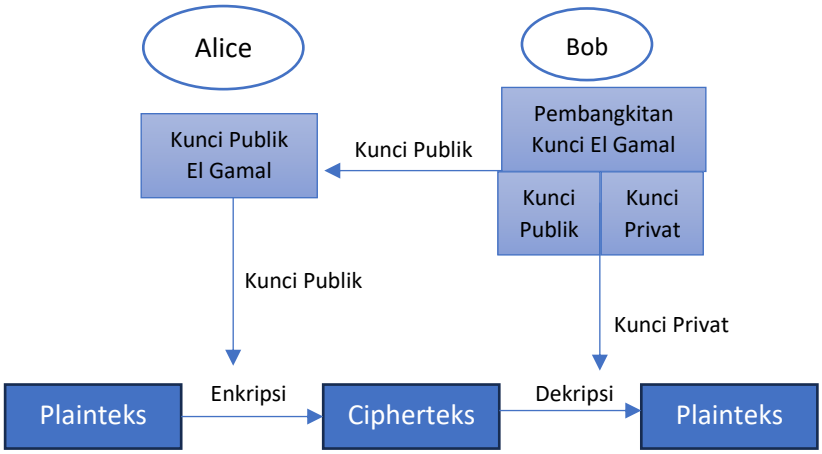
Gambar 3.1 Skema Algoritma *Atbash Cipher*

Skema *autokey cipher* ditunjukkan pada gambar berikut:



Gambar 3.2 Skema Algoritma *Autokey Cipher*

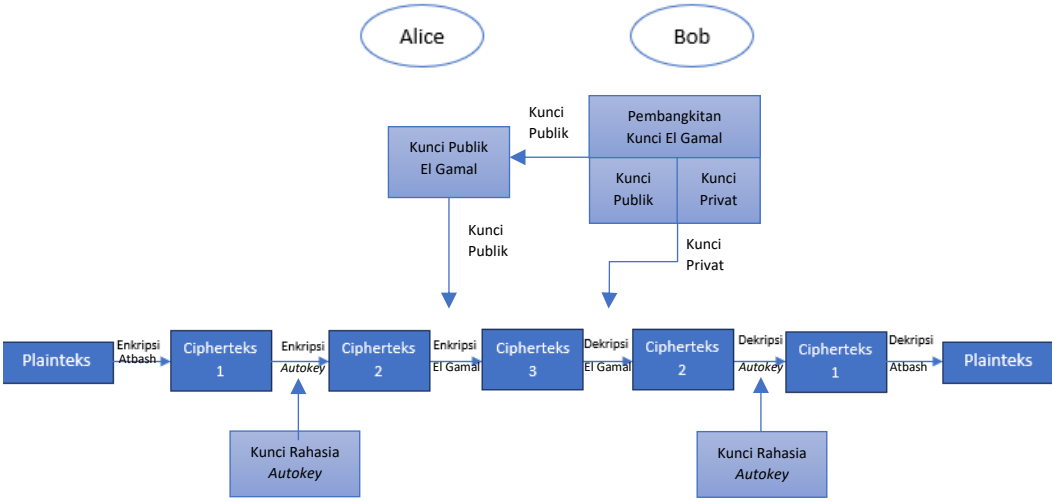
Skema algoritma El Gamal ditunjukkan pada gambar berikut:



Gambar 3.3 Skema Algoritma El Gamal

3.3 Pengembangan Model

Pengembangan model dasar pada penelitian ini yaitu dengan menggabungkan atau mengkombinasi ketiga algoritma yang terdapat pada model dasar sebelumnya, yaitu algoritma *atbash -autokey cipher* dan algoritma El Gamal. Pengkombinasian pada ketiga kriptografi ini disebut sebagai kriptografi *hybrid*. Berikut ini ditunjukkan skema pengembangan pada kriptografi *hybrid* tersebut:



Gambar 3.4 Skema Pengembangan Model

Hal pertama kali yang dilakukan adalah terlebih dahulu membangkitkan kunci privat dan publik menggunakan algoritma El Gamal oleh Bob yang selanjutnya kunci publik tersebut dikirim pada Alice. Kemudian, Alice melakukan proses enkripsi terhadap plainteks menggunakan algoritma *atbash* hingga didapatkan cipherteks 1 yang kemudian dilakukan proses enkripsi lagi dengan kunci rahasia

untuk *autokey cipher* hingga didapatkan cipherteks 2. Akhirnya setelah mendapatkan cipherteks 2, maka dilakukan enkripsi menggunakan algoritma El Gamal hingga didapatkan cipherteks 3.

Untuk tahap pendekripsian cipherteks, mulanya akan dilakukan dekripsi pada cipherteks 3 menggunakan algoritma El Gamal hingga didapatkan cipherteks 2. Selanjutnya, pada cipherteks 2 dilakukan dekripsi lagi dengan algoritma *autokey cipher* hingga didapatkan cipherteks 1, terakhir pada cipherteks 1 dilakukan dekripsi lagi menggunakan algoritma *atbash* sehingga diperoleh plainteks.

3.4 Konstruksi Program

Penelitian ini akan dibuat susunan programnya atau dikonstruksi menggunakan program python berbasis *Graphical User Interface* (GUI). Untuk detail susunan program adalah sebagai berikut:

3.4.1 Input dan Output

Pada proses enkripsi, Alice perlu menginput pesan, kunci publik El Gamal yang terlebih dulu dibangkitkan oleh Bob (p, g dan y), dan kunci rahasia yang nantinya program akan menghasilkan output berupa cipherteks yang telah dienkripsi oleh kriptografi *hybrid* algoritma *atbash-autokey cipher* dan algoritma El Gamal.

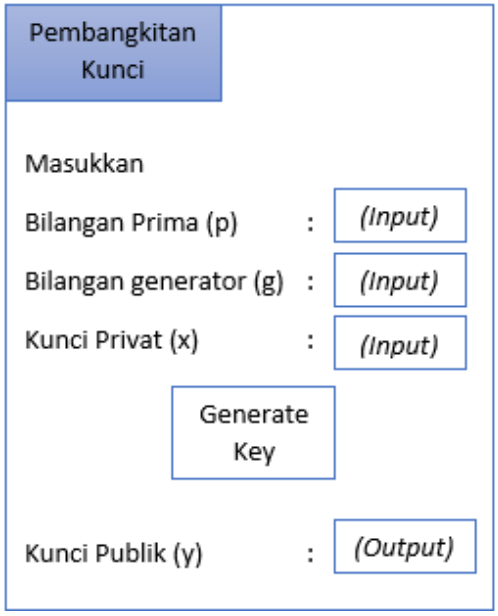
Pada proses pembangkitan kunci El Gamal dan mendekripsi pesan akan dilakukan oleh Bob, sementara Alice akan melakukan proses enkripsi. Pada pembangkitan kunci, Bob perlu melakukan input berupa kunci privat (x, p dan g) yang selanjutnya akan mendapatkan output berupa kunci publik (y). Tetapi, saat proses dekripsi pesan Bob diharuskan menginput cipherteks, bilangan prima dan kunci privat untuk El Gamal, dan kunci rahasia untuk *autokey cipher*, yang selanjutnya akan menghasilkan output adalah plainteks yang berisikan informasi yang ingin disampaikan Alice.

Pada proses pengujian *Avalanche Effect* (AE), perlu untuk input pesan 1 dan 2, kunci rahasia, dan kunci publik (p, y dan g) yang akan menghasilkan output hasil uji dalam persen dan kriterianya. Dengan demikian maka rancangan tampilan pada program aplikasi ini terdapat 4 fungsi utama, yaitu pembangkitan kunci, enkripsi dan dekripsi, serta uji AE.

3.4.2 Rancangan Tampilan Program Aplikasi

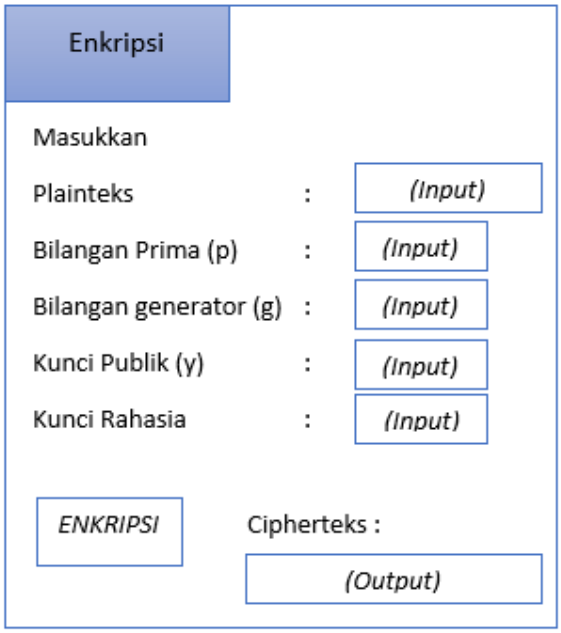
Rancangan dalam tampilan program memiliki 4 menu utama, yaitu yang pertama adalah pembangkitan kunci, untuk menu kedua dan ketiga berturut adalah enkripsi dan dekripsi, dan terakhir menu keempat adalah menu pengujian *Avalanche Effect (AE)*. Berikut ini ditunjukkan rancangan dalam tampilan program yang akan dibuat:

a) Menu Pembangkitan Kunci



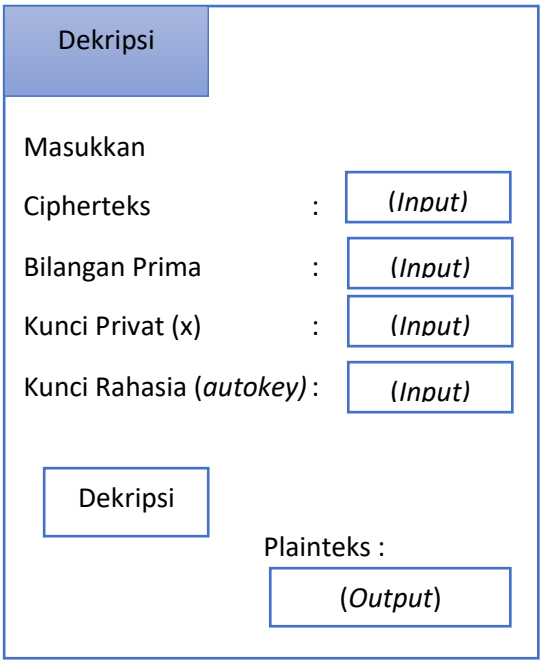
Gambar 3. 5 Rancangan Tampilan Pembangkitan Kunci

b) Menu Enkripsi



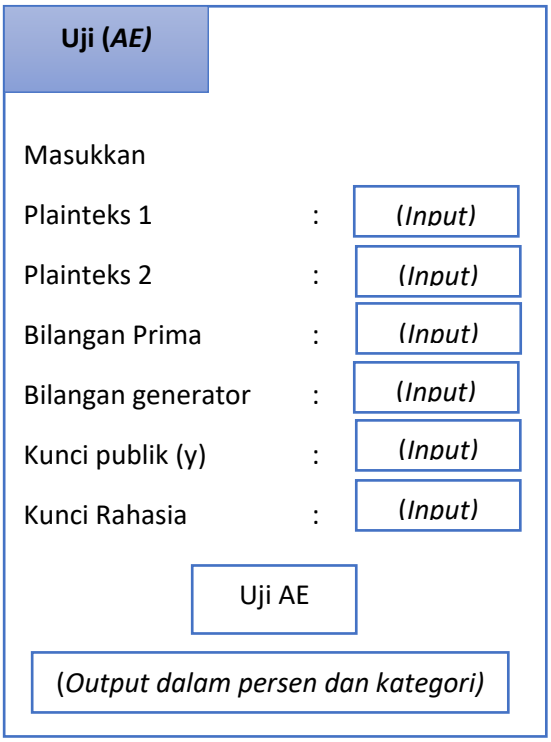
Gambar 3. 6 Rancangan Tampilan Enkripsi

c) Menu Dekripsi



Gambar 3.7 Rancangan Tampilan Dekripsi

d) Menu Pengujian *Avalanche Effect (AE)*



Gambar 3.8 Rancangan Tampilan Pengujian *AE*

3.4.3 Algoritma Deskriptif

Algoritma untuk melakukan proses kriptografi *hybrid* pada aplikasi penelitian ini diuraikan sebagai berikut:

- **Algoritma Pembangkitan Kunci**
  1. Pengguna aplikasi memasukkan bilangan prima (p), generator (g), dan kunci privat (x).
  2. Pengguna menekan tombol "*Generate Key*".
- **Algoritma Enkripsi**
  1. Pengguna memasukkan plainteks
  2. Pengguna memasukkan bilangan prima (p), bilangan generator (g), kunci publik (y).
  3. Pengguna memasukkan kunci rahasia (*autokey*).
  4. Pengguna menekan tombol "Enkripsi".
- **Algoritma Dekripsi**
  1. Pengguna memasukkan cipherteks.
  2. Pengguna memasukkan bilangan prima (p), kunci privat (x).
  3. Pengguna memasukkan kunci rahasia (*autokey*).
  4. Pengguna menekan tombol "Dekripsi".
- **Algoritma uji AE**
  1. Pengguna memasukkan plainteks 1 dan plainteks 2.
  2. Pengguna memasukkan bilangan prima p.
  3. Pengguna memasukkan bilangan generator g.
  4. Pengguna memasukkan kunci publik (y).
  5. Pengguna memasukkan kunci rahasia (*autokey*).
  6. Pengguna menekan tombol "Uji AE".

3.5 Proses Validasi

Untuk tahap validasi akan dilakukan pengecekan dan atau pengujian pada program aplikasi yang telah dirancang sedemikian rupa sehingga validasi akan dilakukan dengan memberi contoh terhadap program aplikasi dan kemudian akan disamakan dengan perhitungan manual. Yang akhirnya program aplikasi akan dikatakan teruji atau valid apabila cipherteks terakhir dapat dikembalikan lagi menjadi

plainteks seperti pada pesan awal (deksripsi berhasil) dan juga untuk perolehan hasil yang didapatkan dari proses enkripsi maupun hasil yang didapatkan dari proses dekripsi pada program sama seperti pada perhitungan manual.

3.6 Pengambilan Kesimpulan

Untuk tahap ini adalah penarikan kesimpulan dari pengembangan terhadap model dasar yang telah dilakukan, yaitu kriptografi *hybrid* antara algoritma *atbash -autokey cipher* dan algoritma El gamal serta hasil uji dengan *Avalanche Effect (AE),* dan penerapannya dalam aplikasi berbasis GUI Python.