BAB III
METODE PENELITIAN

3.1 Model Dasar

Model dasar yang digunakan adalah kurva eliptik, Diffie Hellman, ECC, dan ECDH. ECC merupakan kriptografi asimetris. Keamanan kriptografi asimetris ini didasarkan pada sulitnya memecahkan ECDLP. ECDH merupakan salah satu perluasan dari ECC. ECDH adalah protokol pembuatan kunci rahasia antara dua pihak yang berjauhan, Alice dan Bob (kunci rahasia adalah salah satu titik pada kurva elips). Menurut Munir (2013) mengenai algoritma ECDH dijelaskan sebagai berikut. Misal Alice dan Bob ingin berbagi sebuah kunci rahasia. Alice dan Bob terlebih dahulu menghitung kunci publik dan kunci privat masing-masing.

- Alice
  - ✓ Kunci privat = a
  - ✓ Kunci publik = $P_A = a \times B$
- Bob
  - ✓ Kunci privat = b
  - ✓ Kunci publik = $P_B = b \times B$

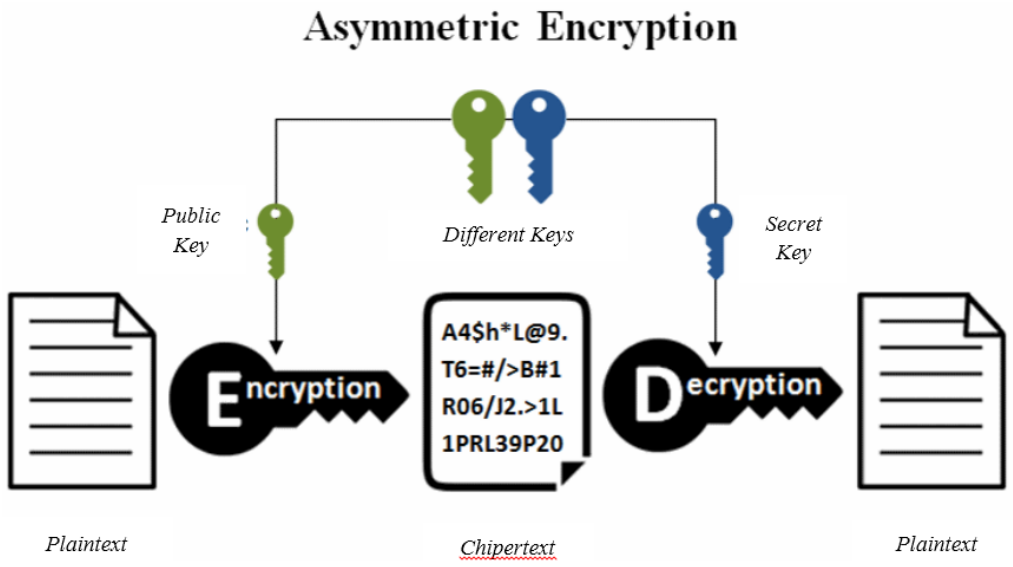
Setelah itu Alice dan Bob saling mengirim kunci publik masing-masing. Kemudian keduanya melakukan perkalian kunci privatnya dengan kunci publik mitranya untuk mendapatkan kunci rahasia yang mereka bagi.

- Alice $\longrightarrow K_{AB} = a(bB)$
- Bob $\longrightarrow K_{AB} = b(aB)$
- Kunci rahasia $K_{AB} = abB = baB$

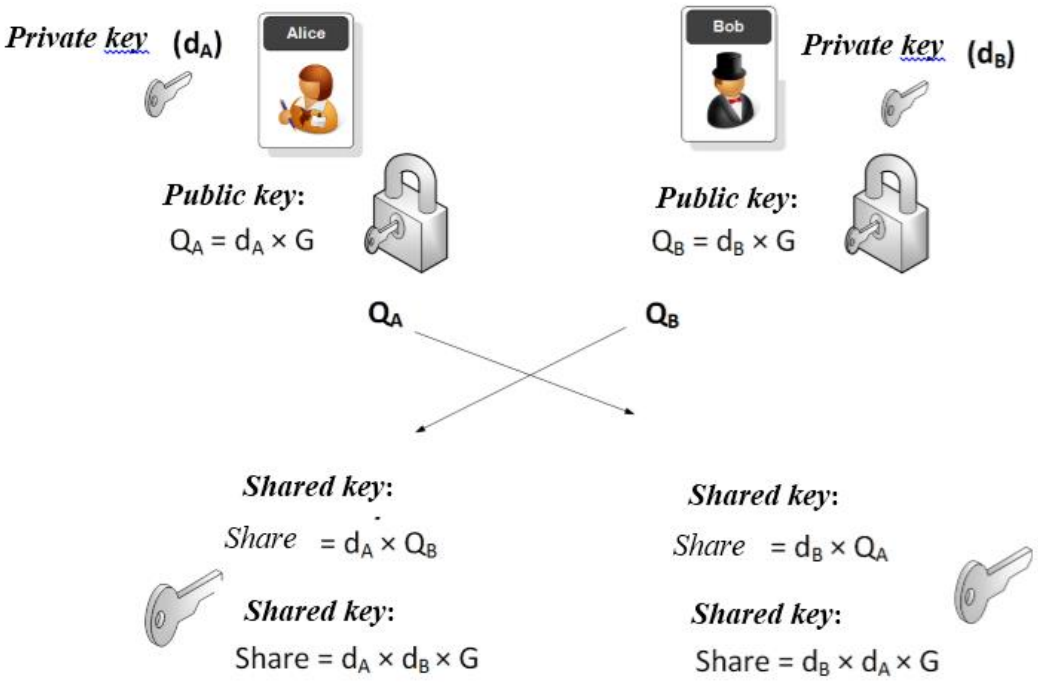
Contoh 5:

Misalkan Alice ingin mengirim email kepada Bob. Alice dan Bob harus menyepakati Kurva Elips (E : $y^2 = (x^3 + x + 1) \bmod 5$) dan titik elips pada E sebagai generator P(0,1). Alice menentukan kunci privat (ka=3) dan Bob menentukan kunci privat (kb=7). Alice menghitung kunci public X= ka . P = 3P=(2,1) dan Bob menghitung kunci public Y= kb . P = 7P=(4,3). Alice dan Bob bertukar kunci publik.). Alice dan Bob bertukar kunci publik. Alice menghitung kunci simetris K= ka .Y = 3 .(7P) = 21P=3P=(2,1) dan Bob

menghitung kunci simetris K= kb . X = 7 . (3P)= 21P=3P=(2,1). Berikut ilustrasi untuk menggambarkan algoritma ECC menurut Nakov (2018) dan algoritma ECDH menurut Buchanan (2020).



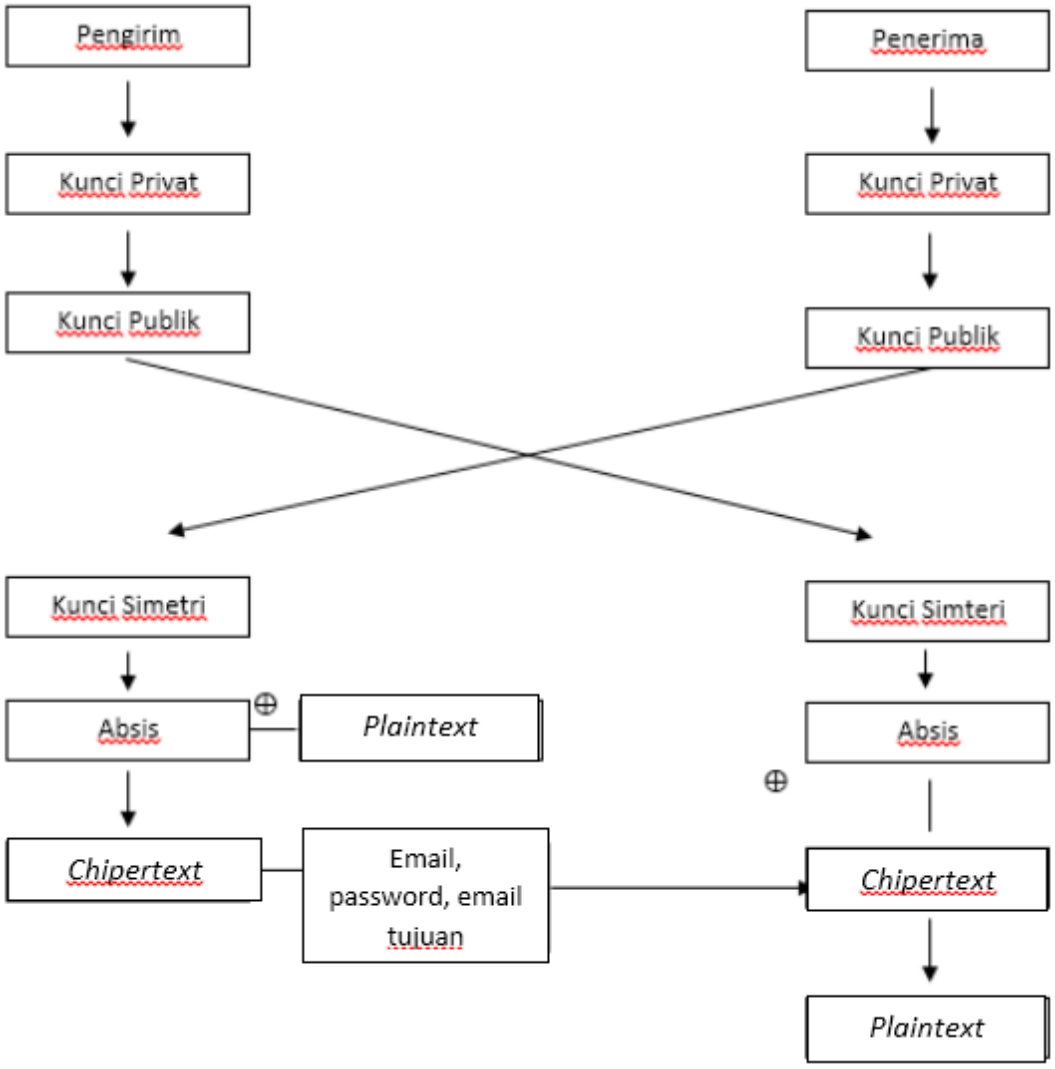
Gambar 3. 1 Algoritma ECC



Gambar 3. 2 Algoritma ECDH

3.2 Pengembangan Model

Pada penelitian ini akan dirancang sebuah aplikasi pengirim email. Tujuannya adalah untuk mengamankan isi pesan email. Langkah pertama adalah membuat kunci simetri bersama dengan protokol ECDH. Setelah mendapatkan kunci simetri yang berupa titik kurva elips, ambil absis dari kunci simetri tersebut yang nantinya akan digunakan untuk mengenkripsi pesan. Proses enkripsinya yaitu dengan cara mengeserkan setiap karakter pada pesan dengan absis dari kunci simetri dengan menggunakan Cipher Caesar. Setelah dienkripsi, kirim *chipertext* tersebut ke penerima pesan. Untuk proses dekripsi, *chipertext* didekripsi dengan kunci yang sama dengan kunci enkripsi. Berikut gambar yang menjelaskan skema pengembangan ECDH untuk enkripsi email.



Gambar 3. 3 Skema pengembangan ECDH untuk enkripsi email

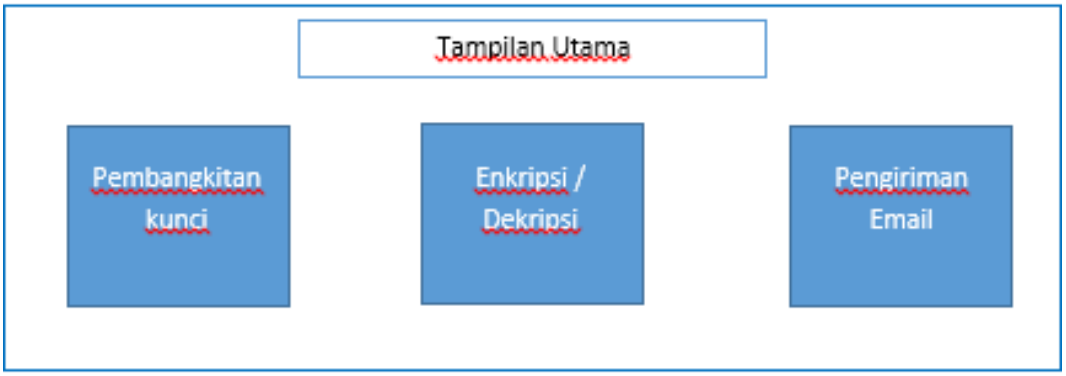
3.3 Perancangan Program Komputer

Program yang akan dibuat memiliki tampilan awal (menu utama) yang memiliki tiga pilihan, yaitu kirim Email, pembangkitan kunci simeteri menggunakan protokol ECDH, dan enkripsi atau dekripsi Email.

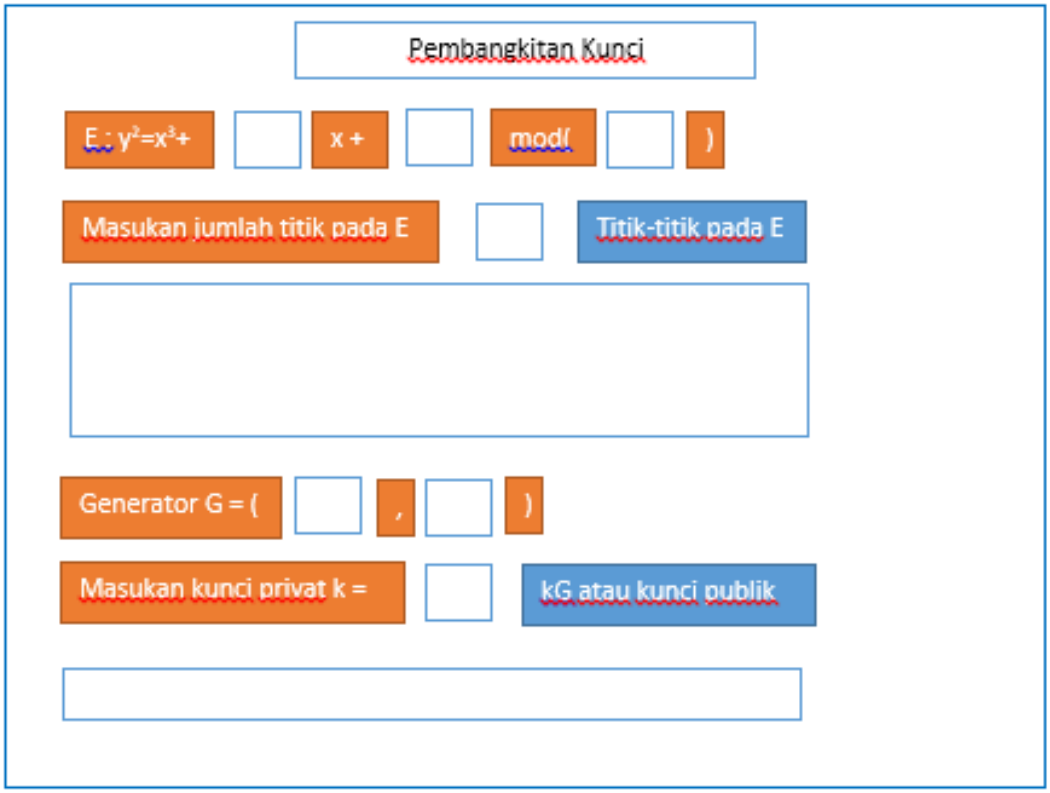
3.3.1 Input Output

Program aplikasi yang dibuat memiliki fungsi untuk melakukan pembangkitan kunci, enkripsi atau dekripsi, dan pengiriman email. Data atau pesan berupa *text alfanumerik* yang diinputkan secara manual ke dalam aplikasi pengirim email. Input dari pembangkitan kunci meliputi kurva elips, order G, dan kunci privat. Output dari pembangkitan kunci yaitu kunci simetris yang digunakan untuk enkripsi dan dekripsi. Input dari enkripsi atau dekripsi meliputi data atau pesan (*plaintext* atau *chipertext*) dan kunci simetris. Output dari enkripsi atau dekripsi adalah *chipertext* atau *plaintext*. Input dari pengiriman email meliputi email pengirim, password email pengirim, email tujuan, subjek email, dan pesan email. Output dari pengiriman email yaitu tulisan ‘pesan sukses terkirim’.

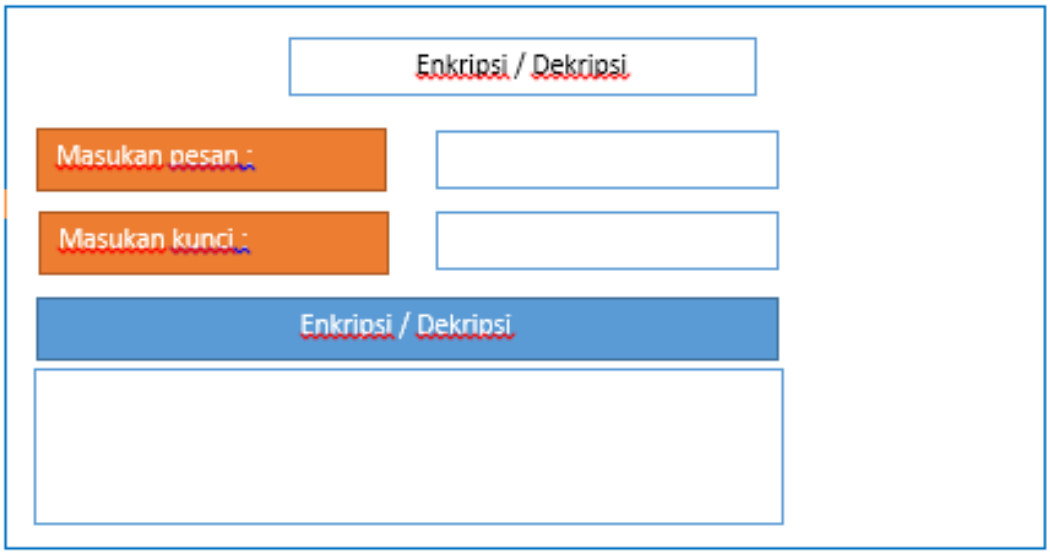
3.3.2 Rancangan Tampilan



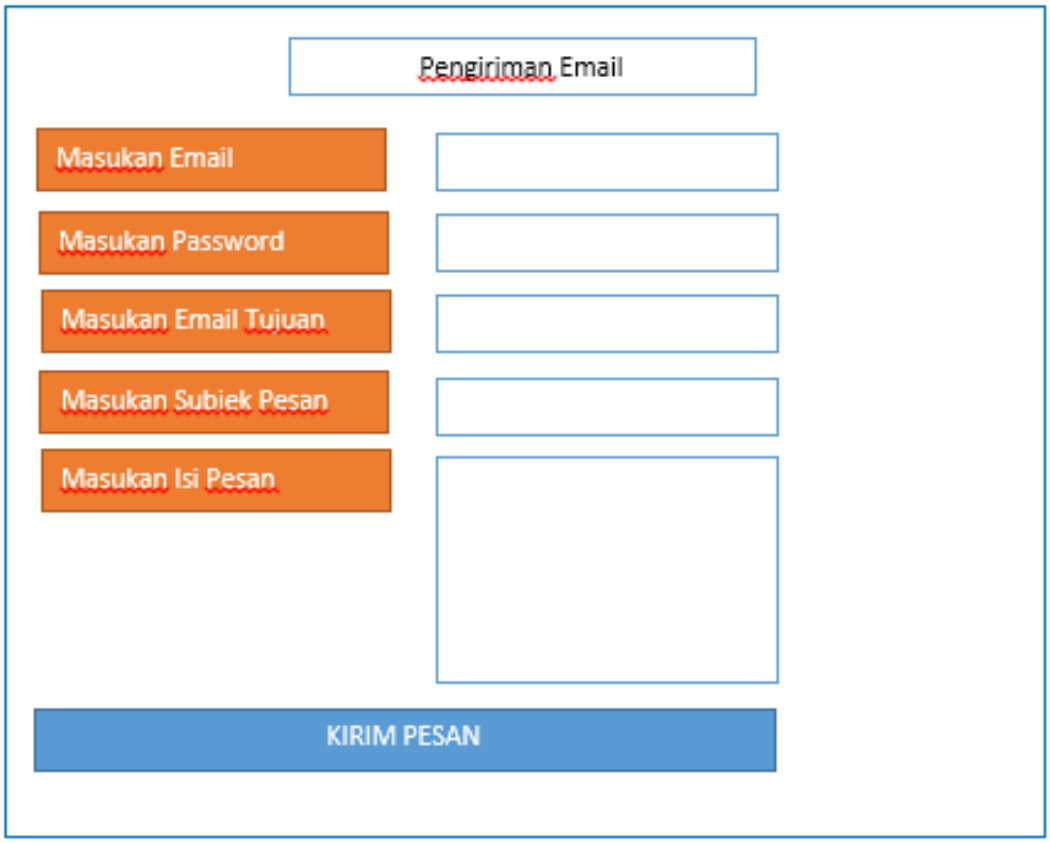
Gambar 3. 4 Tampilan Utama



Gambar 3. 5 Pembangkitan Kunci



Gambar 3. 6 Enkripsi dan Dekripsi



Gambar 3. 7 Pengiriman Email

3.4 Algoritma

3.4.1 Pembangkitan Kunci:

- Tetapkan kurva
- Pilih generator
- Pilih kunci privat (pengirim dan penerima)
- Bangkitkan kunci publik
- Tukar kunci publik
- Bangkitkan kunci simetri
- Output (*a, b)*
- Ambil absis dari output untuk kunci enkripsi atau dekripsi

3.4.2 Enkripsi:

Langkah-langkah:

1. Pengirim pesan memasukkan pesan yang akan dikirim tanpa menggunakan spasi dan huruf kecil semua (*plaintext*).
2. Sebuah kunci simetri akan diberikan pada pengirim.
3. Pengirim mengenkripsi *plaintext* dengan kunci simetri (*ciphertext*).

Algoritma:

- Masukan *plaintext*
- Masukan kunci
- *Ciphertext* = *plaintext* + kunci
- Print *Ciphertext*

3.4.3 Pengiriman email

Langkah-langkah:

1. Pengirim pesan memasukkan emailnya, password emailnya, email tujuan, Subjek pesan, isi pesan (*ciphertext*).
2. Pengirim pesan mengirim *ciphertext* ke email tujuan.

Algoritma:

- Login email
- Masukan subjek
- Masukan *ciphertext*
- Masukan email tujuan
- Kirim email

3.4.4 Dekripsi

Langkah-langkah:

1. Penerima pesan memasukkan pesan yang didapat melalui emailnya, setelah itu mencopykan isi pesan (*ciphertext*) tersebut ke aplikasi dekripsi.
2. Sebuah kunci simetri akan diberikan pada penerima.
3. Penerima mengdekripsi *chipertext* dengan kunci simetri (*plaintext*).

Dekripsi:

- Masukan *ciphertext*
- Masukan kunci
- *Plaintext* = *ciphertext* + kunci
- Print *Plaintext*

3.5 Validasi

Skema pengiriman email dengan ECDH yang diperoleh akan diperikas validasinya terhadap program yang dikonstruksi. Validasi dilakukan untuk mengetahui apakah skema yang dirancang sudah sesuai atau belum.

Setelah skema divalidasi, maka email yang dikirim melalui aplikasi pengirim email menggunakan ECDH akan lebih sulit diretas ketimbang mengirim email tanpa dienkripsi terlebih dahulu.