V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini berhasil menerapkan kriptosistem kurva eliptil ElGamal untuk mengamankan data pribadi berupa alamat pada Kartu Tanda Penduduk (KTP) yang berbentuk teks.

1. Implementasi dilakukan dengan mengubah plainteks ke dalam bentuk desimal ASCII kemudian menggunakan metode Koblitz untuk mengonversi nilai desimal ASCII menjadi titik-titik pada kurva eliptik, sehingga data dapat direpresentasikan dalam bentuk matematis yang tidak dapat dibaca.

   Langkah-langkah utama dalam proses enkripsi kriptosistem kurva eliptik ElGamal meliputi:

   a. Pemilihan parameter pada kriptosistem meliptui bilangan prima $p = 997$, serta nilai $a = 6$ dan $b = 4$. Dengan demikian, diperoleh bentuk kurva eliptik $y^2 = x^3 + 6x + 4$, dengan titik basis $B = (0,2)$.
   b. Memilih kunci priva $d = 2$ dan menghitung kunci publik $e = d \cdot B = 2(0,2) = (750,867)$.
   c. Proses enkripsi, di mana setiap plainteks yang telah direpresentasikan sebagai titik pada kurva eliptik dienkripsi menggunakan kriptosistem kurva eliptik ElGamal, menghasilkan cipherteks berupa pasangan titik-titik pada kurva eliptik yang tidak dapat dimengerti tanpa kunci privat.

   Dengan proses tersebut, sistem berhasil mengubah data teks berupa alamat pada Kartu Tanda Penduduk (KTP) menjadi representasi matematis yang aman, sehingga membuktikan bahwa kriptosistem kurva eliptik ElGamal efektif dalam menjaga kerahasiaan data pribadi.
2. Proses dekripsi dilakukan untuk mengembalikan cipherteks menjadi plainteks semula dengan menggunakan kunci privat yang telah dibangkitkan sebelumnya.

   Langkah-langkah dekripsi pada penelitian ini meliputi:

   a. Mengalikan kunci privat $d = 2$ dengan *ephemeral key*.
   b. Kemudian mengurangkan *ciphertext part* dengan hasil kali kunci privat dengan *ephemeral key*.
   c. Mengembalikan titik hasil dekripsi menjadi representasi desimal ASCII melalui dekoding dengan metode Koblitz.
   d. Mengonversi kembali nilai desimal ASCII ke bentuk karakter teks, sehingga diperoleh kembali data plainteks semula.

Hasil dekripsi menunjukkan bahwa kriptosistem kurva eliptik ElGamal berhasil merekonstruksi plainteks “001 Lagan Ulu” secara tepat, tanpa adanya kehilangan

atau perubahan data. Hal ini membuktikan bahwa proses enkripsi dan dekripsi dalam kriptosistem kurva eliptik ElGamal telah berjalan dengan benar dan efisien. Dengan demikian, dapat disimpulkan bahwa kriptosistem ElGamal berbasis kurva eliptik mampu menjaga keutuhan serta kerahasiaan data teks pribadi, sekaligus menawarkan efisiensi yang lebih tinggi dibandingkan sistem non-eliptik dengan tingkat keamanan yang setara. Selain itu, penggunaan metode Koblitz memberikan cara sistematis dan akurat untuk merepresentasikan data ASCII sebagai titik valid pada kurva eliptik.

5.2 Saran

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, penulis menyadari bahwa masih terdapat beberapa keterbatasan dalam penelitin ini. Oleh karena itu, penulis memberikan beberapa saran yang diharapkan dapat menjadi bahan pertimbangan dan acuan untuk penelitian selanjutnya, yaitu:

1. Untuk penelitian berikutnya, diharapkan sistem enkripsi dan dekripsi berbasis kriptosistem kurva eliptik ElGaml dapat diimpelentasi dalam bentuk program komputer, sehingga dapat dilakukan perbandingan hasil antara perhitungan manual dan hasil program.
2. Dalam implementasi kriptosistem kurva eliptik ElGamal untuk pertukaran pesan, disarankan untuk mempertimbangkan metode pengkodean alternatif selain metode Koblitz, karena metode Koblitz memerlukan proses pencarian titik representasi dari data ASCII yang mengurangi efisiensi perhitungan secara manual.
3. Meningkatkan tingkat keamanan sistem dengan menggunakan bilangan prima yang lebih besar, karena hal tersebut akan memperbesar kompleksitas perhitungan logaritma diskrit pada kurva eliptik, sehingga memperkuat ketahanan kriptosistem terhadap berbagai jenis serangan.