RINGKASAN

Penelitian ini membahas penerapan kriptosistem kurva eliptik ElGamal sebagai metode pengamanan data pribadi pada Kartu Tanda Penduduk (KTP). Latar belakang penelitian ini didorong oleh meningkatnya kasus kebocoran dan penyalahgunaan data pribadi di Indonesia. Tujuan penelitian adalah untuk menerapkan algoritma kriptografi berbasis kurva eliptik guna melakukan proses enkripsi dan dekripsi terhadap data teks berupa alamat pada KTP, dengan menggunakan metode Koblitz untuk mengubah karakter ASCII menjadi titik-titik pada kurva eliptik.

Implementasi dilakukan pada kurva eliptik $y^2 = x^3 + 6x + 4$ di atas lapangan hingga modulo bilangan prima $p = 997$, dengan titik basis $B = (0,2)$, kunci privat $d = 2$, dan kunci publik $e = dB = (750,867)$. Proses enkripsi menghasilkan cipherteks berupa pasangan titik pada kurva eliptik yang tidak dapat dibaca tanpa kunci dekripsi, sedangkan proses dekripsi berhasil mengembalikan plainteks ke bentuk semula.

Hasil penelitian menunjukkan bahwa kriptosistem kurva eliptik ElGamal mampu memberikan tingkat keamanan tinggi dengan ukuran kunci yang relatif kecil, sehingga efisien dalam penggunaan memori dan waktu komputasi. Metode Koblitz terbukti dapat mengubah plainteks menjadi titik pada kurva secara valid, meskipun memerlukan waktu pencarian yang cukup lama.

Penulis menyarankan agar penelitian selanjutnya mengembangkan sistem ini dalam bentuk program komputer untuk membandingkan hasil manual dan hasil program, serta mempertimbangkan metode enkoding alternatif selain Koblitz guna meningkatkan efisiensi. Selain itu, penggunaan bilangan prima yang lebih besar dan variasi parameter kurva eliptik direkomendasikan untuk memperkuat keamanan sistem.

SUMMARY

This research discusses the implementation of the Elliptic Curve ElGamal Cryptosystem as a method to secure personal data on the Indonesian Identity Card (KTP). The study is motivated by the increasing number of data breaches and misuse of personal information in Indonesia. The objective of this research is to apply the elliptic curve–based cryptographic algorithm to perform encryption and decryption processes on textual data—specifically, the address information contained in the KTP—using the Koblitz method to convert ASCII characters into points on an elliptic curve.

The implementation was carried out on the elliptic curve $y^2 = x^3 + 6x + 4$ *over a finite field modulo a prime number* $p = 997$*, with base point* $B = (0,2)$*, private key* $d = 2$*, and public key* $e = dB = (750,867)$*. The encryption process produced ciphertexts in the form of point pairs on the elliptic curve that cannot be read without the private key, while the decryption process successfully recovered the original plaintext.*

The results show that the Elliptic Curve ElGamal Cryptosystem provides a high level of security with relatively small key sizes, making it efficient in terms of memory usage and computational performance. The Koblitz method effectively converts plaintext into valid curve points, although it requires an extensive search process.

For future work, it is recommended to develop the system into a computer-based application to compare manual and programmatic results, and to consider alternative encoding methods other than Koblitz to improve system efficiency. Additionally, using larger prime numbers and varying elliptic curve parameters are suggested to enhance the cryptographic strength.