KRIPTOSISTEM DENGAN MODIFIKASI *ELLIPTIC CURVE CRYPTOGRAPHY*

Nama : Muhamamad Firdhausi Fahmi
NIM : 02201010
Dosen Pembimbing Utama : Aditya Putra Pratama, S.Si., M.Si.
Pembimbing Pendamping : Yanuar Bhakti Wira Tama, S.Si., M.Si.

ABSTRAK

Keamanan data telah menjadi hal yang sangat krusial dalam dunia digital saat ini. Dalam upaya melindungi data dari akses yang tidak diinginkan, kriptografi memiliki peran sentral untuk mengamankan kerahasiaan data. Kriptografi memanfaatkan berbagai metode, termasuk metode simetris dan asimetris, dengan menggunakan kunci enkripsi dan dekripsi. Salah satu metode kriptografi asimetris adalah *Elliptic Curve Cryptography* (ECC). Beberapa penelitian sebelumnya menyimpulkan bahwa ECC efektif untuk meningkatkan keamanan data dari ancaman akses luar. Penelitian ini berfokus pada modifikasi ECC untuk menciptakan kriptosistem dari pemilihan parameter kurva eliptik. Tujuan utamanya adalah mengetahui bahwa ECC dapat meningkatkan tingkat keamanan data. Penentuan kurva eliptik, definisi elemen kriptosistem, komputasi, analisis hasil, dan kesimpulan menjadi tahapan penting dalam penelitian ini. Penelitian ini dapat memberikan kontribusi berharga dalam pengembangan teknologi kriptografi dalam mengamankan data penting dari ancaman luar yang berbahaya. Dengan demikian, penelitian ini memiliki dampak dalam menjaga privasi dan keamanan dengan menggunakan *Elliptic Curve Cryptography*. Adapun kesimpulan dari penelitian ini yaitu dalam pemilihan kurva eliptik dalam performa *running time* proses ECC tidak berpengaruh secara signifikan, dimana dalam proses enkripsi dengan *range* 2.7-11.08 *milisecond* dan dekripsi dengan *range* 2.7-6.93 *milisecond* dalam *Elliptic Curve Cryptography* yang artinya bahwa pemilihan parameter dalam ECC memiliki proses yang singkat di setiap parameter.

Kata kunci: *ECC, keamanan data, kurva eliptik, kriptografi, kriptosistem*