ABSTRAK

Nama : **Ristati Novitadini**

NIM : **1197010063**

Judul Skripsi : **Modifikasi Algoritma *Linear Block Cipher* dengan Kunci Simetris Sederhana melalui Pembangkitan *Round Key***

Algoritma kriptografi simetris seperti *Linear Block Cipher* dan Kunci Simetris Sederhana memiliki mekanisme enkripsi yang relatif sederhana dan menggunakan operasi aritmetika modular. Namun, penggunaan algoritma secara tunggal memiliki struktur enkripsi yang terbatas, sehingga diperlukan pengembangan melalui kombinasi beberapa mekanisme enkripsi untuk menghasilkan proses pengamanan data yang lebih kompleks. Penelitian ini bertujuan memodifikasi algoritma *Linear Block Cipher* dengan Kunci Simetris Sederhana melalui penerapan enkripsi berlapis serta pembangkitan *round key* untuk setiap blok data. Metode penelitian meliputi perancangan algoritma, pembangkitan kunci, proses enkripsi dan dekripsi, serta simulasi menggunakan data teks. *Plaintext* direpresentasikan dalam ASCII 8-bit, kemudian dienkripsi menggunakan *Linear Block Cipher* melalui perkalian matriks kunci pada modulo 256 dan dilanjutkan dengan Kunci Simetris Sederhana menggunakan $k_{1,i}$ dan $k'_{2,i}$. Proses dekripsi dilakukan dengan membalik tahapan enkripsi menggunakan invers modular dan invers matriks kunci. Hasil penelitian menunujukkan bahwa kombinasi kedua algoritma menghasilkan *ciphertext* melalui dua tahap enkripsi dan dapat dikembalikan menjadi *plaintext* semula menggunakan kunci yang sesuai. Dengan demikian, modifikasi algoritma yang diusulkan dapat diterapkan sebagai skema enkripsi berlapis untuk menghasilkan proses pengamanan data yang lebih kompleks dibandingkan penggunaan algoritma secara tunggal.

Kata kunci: kriptografi simetris, *Linear Block Cipher*, Kunci Simetris Sederhana, *round key*, modulo 256, enkripsi, dekripsi.

ABSTRACT

Name **: Ristati Novitadini**

NIM **: 1197010063**

Title **: *Modification of the Linear Block Cipher Algorithm with a Simple Symmetric Key through Round Key Generation***

Symmetric cryptographic algorithms such as Linear Block Cipher and Simple Symmetric Key have relatively simple encryption mechanisms and use modular arithmetic operations. However, using a single algorithm has a limited encryption structure; therefore, combining multiple mechanisms is needed to produce a more complex data protection process. This study aims to modify both algorithms through layered encryption and round key generation for each data block. The research methods include algorithm design, key generation, encryption and decryption processes, and simulation using text data. The plaintext is represented in 8-bit ASCII, then encrypted using Linear Block Cipher through matrix-key multiplication modulo 256, followed by Simple Symmetric Key encryption using $k_{1,i}$ *and* $k'_{2,i}$*. The decryption process is performed in reverse using the modular inverse and the inverse of the key matrix. The results show that the combination of the two algorithms produces ciphertext through two encryption stages and can be restored to the original plaintext using the corresponding keys. Therefore, the proposed method can be applied as a layered encryption scheme to produce a more complex data protection process than using a single algorithm.*

Keywords: symmetric cryptography, Linear Block Cipher, Simple Symmetric Key, round key, modulo 256, encryption, decryption.