ABSTRAK

Nama : **Zidan Ahamada**

NIM : **1207010082**

Judul Skripsi : **Algoritma El-Gamal Pada Teknik Kriptografi Affine-Hill Cipher dengan Pembangkit Kunci Matriks Multinacci.**

Skripsi ini membahas kriptografi kunci publik yang menggabungkan dua cipher klasik, yaitu Affine cipher dan Hill cipher, yang dikenal dengan istilah Affine-Hill cipher, menggunakan matriks Fibonacci yang diperumum, atau matriks multinacci. Penelitian ini mengusulkan skema pembentukan kunci inovatif yang melibatkan pertukaran matriks kunci $K = Q_\lambda^k$ dari orde $\lambda x \lambda$ untuk enkripsi dan dekripsi, dengan bantuan barisan multinacci di bawah modulo utama. Barisan multinacci ini memungkinkan pembentukan kunci yang lebih variatif dan sulit ditebak, sehingga meningkatkan keamanan skema kriptografi yang diusulkan. Salah satu keunggulan utama dari skema ini adalah efisiensi dalam pertukaran kunci, di mana hanya perlu menukar pasangan angka (λ, k) sebagai pengganti seluruh matriks kunci, yang mengurangi kompleksitas waktu dan ruang. Selain itu, skema ini juga menyediakan ruang kunci yang besar, memperluas kemungkinan kombinasi kunci yang dapat digunakan, dan meningkatkan keamanan enkripsi secara keseluruhan. Dengan demikian, penelitian ini tidak hanya mengusulkan metode baru dalam kriptografi kunci publik, tetapi juga menawarkan solusi yang lebih efisien dan aman untuk proses enkripsi dan dekripsi data.

Kata Kunci: Affine-Hill cipher, Kriptografi, barisan dan matriks Fibonacci, barisan & matriks Multinacci.

ABSTRACT

Name : **Zidan Ahamada**

NIM : **1207010082**

Title :**El-Gamal Algorithm on Affine-Hill Cipher Cryptography Technique with Multinacci Matrix Key Generator.**

This thesis discusses public key cryptography that combines two classical ciphers, namely Affine cipher and Hill cipher, known as Affine-Hill cipher, using a generalized Fibonacci matrix, or multinacci matrix. This research proposes an innovative key establishment scheme that involves exchanging key matrices $K = Q_{\lambda}^{k}$ *of order* $\lambda x \lambda$ *for encryption and decryption, with the help of multinacci rows under major modulo. These multinacci rows allow for the generation of keys that are more varied and difficult to guess, thus enhancing the security of the proposed cryptographic scheme. One of the main advantages of this scheme is the efficiency in key exchange, where it is only necessary to exchange pairs of numbers (λ,k) instead of the entire key matrix, which reduces the time and space complexity. In addition, this scheme also provides a large key space, expanding the possible key combinations that can be used, and improving the overall encryption security. Thus, this research not only proposes a new method in public-key cryptography, but also offers a more efficient and secure solution for data encryption and decryption processes.*

Keywords: Affine-Hill cipher, Cryptography, Fibonacci sequence and matrix, Multinacci matrix.