KRIPTOGRAFI *HYBRID* METODE HILL CIPHER DAN ELGAMAL DALAM MENINGKATKAN KEAMANAN PESAN RAHASIA

Oleh

Faizar Rusyadi, NIM 1813101027

Jurusan Matematika

ABSTRAK

Perkembangan teknologi informasi telah mengubah cara manusia bertukar informasi, tetapi meningkatkan risiko keamanan terhadap data sensitif. Untuk mengatasi tantangan ini, kriptografi menjadi pendekatan yang efektif dengan mengubah pesan menjadi bentuk yang tidak dapat dibaca tanpa kunci yang tepat. Salah satu teknik kriptografi yang digunakan adalah Hill cipher, yang menggunakan matriks sebagai kunci untuk mengenkripsi dan mendekripsi teks. Meskipun Hill cipher menawarkan kecepatan dalam enkripsi, keamanannya masih rentan terhadap serangan tertentu. Oleh karena itu, penelitian ini mengusulkan pendekatan kriptografi *hybrid* yang menggabungkan kriptografi Hill cipher dengan kriptografi ElGamal untuk meningkatkan tingkat keamanan informasi. Tujuan dari penelitian ini adalah untuk membandingkan kinerja antara Hill cipher, Elgamal, dan metode *hybrid* dalam hal keamanan informasi, serta untuk memahami proses enkripsi dan dekripsi dari ketiga metode tersebut. Metode yang digunakan meliputi studi pustaka untuk memahami landasan teori dan pengembangan model dasar implementasi menggunakan Java NetBeans 18 dengan JDK 20, dengan menganalisis enkripsi 100 data siswa yang dibagi menjadi 34 kategori berdasarkan ukuran karakter. Temuan utama menunjukkan bahwa metode *hybrid* menghasilkan nilai entropi rata-rata tertinggi 7,94, menunjukkan tingkat *randomness* ciphertext yang lebih baik dibandingkan dengan metode Hill cipher dan Elgamal. Namun demikian, metode *hybrid* membutuhkan waktu enkripsi dan dekripsi yang lebih lambat dibandingkan dengan Hill Cipher dan ElGamal. Kesimpulan dari penelitian ini adalah bahwa dalam kasus penggunaan ukuran data yang relatif kecil, metode kriptografi *hybrid* menawarkan keseimbangan yang baik antara keamanan dan kinerja, memberikan potensi alternatif untuk meningkatkan keamanan data dalam lingkungan digital yang terus berkembang.

Kata-kata kunci : Kriptografi, Hill Cipher, Elgamal, *Hybrid*, entropi.

HYBRID CRYPTOGRAPHY OF HILL CIPHER AND ELGAMAL METHOD IN ENHANCING SECRET MESSAGE SECURITY

By

Faizar Rusyadi, NIM 1813101027

Department of Mathematics

ABSTRACT

The development of information technology has changed the way of human's information exchange, but in other hand it also increased the security risks to a sensitive data. Based on that problem, To overcome it, cryptography becomes an effective approach by converting messages into an unreadable form without the right key. One of the cryptographic techniques used is the Hill cipher technique, which uses a matrix as a key to encrypt and decrypt text. Although. Hill cipher offers speed in its encryption, its security is still vulnerable to certain attacks. Therefore, this study analyzes a hybrid approach that combines Hill cipher with ElGamal cryptography in order to inhancing the level of information's security. Which its becoming the purpose of this study with objectively to compare the performance between Hill cipher, Elgamal, and hybrid methods in terms of information security as well as to understand the encryption and decryption process of those three methods. The method used is involving the literatures study to understand the theory and development of a basic model for the implementation of using Java NetBeans 18 with JDK 20. According to the analyzing of the encryption of a hundred students' data. Those are divided into 34 categories based on character size. The main findings showed that the hybrid method produced the highest average entropy value of 7.94, which is indicating a better level of ciphertext randomness than the Hill cipher and Elgamal methods. Nevertheless, the hybrid method requires slower encryption and decryption times than Hill cipher and ElGamal. The conclusion of this study is the case of using relatively small data sizes, hybrid cryptography methods offer a good balance on its security and performance, which is providing alternative potential to inhancing data security in an ever-evolving digital environment.

Keywords: Cryptography, Hill Cipher, Elgamal, Hybrid, entropy