

SUATU SKEMA ENKRIPSI BERBASIS GRAF

Oleh

Ni Putu Permatasari, NIM 2013101024

Jurusan Matematika

ABSTRAK

Kriptografi adalah ilmu dan seni mengamankan informasi dengan mengubahnya menjadi format yang tidak dapat dibaca oleh orang yang tidak berwenang, menggunakan teknik dan algoritma untuk menyandikan (enkripsi) dan mengembalikan (dekripsi) data. Penelitian ini bertujuan untuk membandingkan dua metode kriptografi yang dikembangkan oleh peneliti, yaitu metode 1 dan metode 2. Evaluasi penelitian ini mencakup aspek kompleksitas algoritma, keamanan data, efisiensi, dan kualitas enkripsi-dekripsi. Penelitian dilakukan melalui uji coba kedua metode dengan menggunakan plainteks yang sama dan peneliti menggunakan perangkat lunak untuk mencatat waktu yang dibutuhkan dalam melakukan enkripsi maupun dekripsi. Hasil evaluasi menunjukkan bahwa metode 1 lebih efisien dari segi waktu, tetapi kurang sesuai untuk data yang membutuhkan keamanan tinggi. Sementara itu, metode 2 lebih unggul dalam hal keamanan, namun dengan biaya waktu yang lebih besar dan kompleksitas yang lebih tinggi. Kesimpulan dari penelitian ini adalah bahwa pemilihan pada metode kriptografi harus mempertimbangkan kebutuhan spesifik dari pengguna, terutama terkait dengan keseimbangan antara efisiensi dan keamanan. Untuk penelitian selanjutnya, disarankan untuk mengembangkan metode kriptografi yang dapat menggabungkan keunggulan dari kedua metode ini, sehingga dapat menawarkan keamanan yang tinggi dengan efisiensi yang lebih baik.

Kata kunci: kriptografi, enkripsi, dekripsi, kompleksitas algoritma, keamanan data

A GRAPH-BASED ENCRYPTION SCHEME

by Ni Putu Permatasari, NIM 2013101024

Mathematics

ABSTRACT

Cryptography is the science and art of securing information by converting it into a format that cannot be read by unauthorized persons, using techniques and algorithms to encode (encrypt) and restore (decrypt) data. This study aims to compare two cryptographic methods developed by researchers, namely method 1 and method 2. The evaluation of this study includes aspects of algorithm complexity, data security, efficiency, and encryption-decryption quality. The study was conducted through testing both methods using the same plaintext and researchers used software to record the time required to perform encryption and decryption. The evaluation results show that method 1 is more efficient in terms of time, but less suitable for data that requires high security. Meanwhile, method 2 is superior in terms of security, but with greater time costs and higher complexity. The conclusion of this study is that the selection of cryptographic methods must consider the specific needs of users, especially related to the balance between efficiency and security. For further research, it is recommended to develop a cryptographic method that can combine the advantages of these two methods, so that it can offer high security with better efficiency.

Keywords: cryptography, encryption, decryption, algorithm complexity, data security