INTISARI

Metaheuristik: Evaluasi Dan Perbaikan Keamanan Kata Sandi Dengan Algoritma Genetika. Penelitian ini bertujuan untuk meningkatkan kekuatan password dengan menggunakan algoritma genetika sebagai pendekatan yang efektif dalam mengatasi masalah keamanan data dan informasi sensitif. Metode penelitian ini melibatkan beberapa tahap, dimulai dari pembentukan populasi awal password dengan karakter acak, evaluasi kekuatan password berdasarkan faktor-faktor seperti panjang password, kompleksitas karakter, huruf besar, dan karakter khusus. Selanjutnya, dilakukan operasi crossover dan mutasi untuk menghasilkan password baru dengan kombinasi karakter yang lebih kuat. Hasil penelitian menunjukkan bahwa algoritma genetika berhasil meningkatkan kekuatan password. Password baru yang dihasilkan melalui proses genetika memiliki estimasi waktu pembobolan yang jauh lebih lama dibandingkan dengan password lama. Pengujian menggunakan layanan eksternal, yakni https://www.passwordmonster.com/, juga mengonfirmasi keberhasilan algoritma genetika dalam menciptakan password yang memenuhi standar kekuatan yang lebih tinggi. Berdasarkan hasil penelitian, dapat disimpulkan bahwa algoritma genetika efektif dalam meningkatkan kekuatan password. Implementasi algoritma genetika dalam proses pembentukan password mampu menghasilkan kombinasi karakter yang lebih kuat, meningkatkan keamanan data pribadi, dan mengurangi risiko kebocoran informasi. Penelitian ini memberikan dorongan untuk pengembangan metode pengamanan informasi yang inovatif dan efektif untuk melindungi data pribadi dari serangan yang tidak diinginkan.

Kata kunci: kekuatan password, algoritma genetika, keamanan informasi, data pribadi, estimasi waktu pembobolan.

ABSTRACT

Metaheuristik: Password Security Evaluation And Improvement With Genetics Algorithm. This research aims to improve password strength by using genetic algorithms as an effective approach in addressing data security issues and sensitive information. The research method involves several stages, starting from the formation of an initial population of passwords with random characters, evaluation of password strength based on factors such as password length, character complexity, capitalization, and special characters. Next, crossover and mutation operations are performed to generate new passwords with stronger character combinations. The results show that genetic algorithms can successfully improve password strength. The new password generated through the genetic process has a much longer estimated break-in time compared to the old password. Tests using an external service, namely https://www.passwordmonster.com/, also confirmed the success of genetic algorithms in creating passwords that meet higher strength standards. Based on the research results, it can be concluded that genetic algorithms are effective in increasing password strength. The implementation of genetic algorithms in the password formation process is able to produce stronger character combinations, improve personal data security, and reduce the risk of information leakage. This research provides impetus for the development of innovative and effective information security methods to protect personal data from unwanted attacks.

Keywords: password strength, genetic algorithm, information security, personal data, estimated time to breach.