

INTISARI

Perkembangan teknologi informasi yang sangat pesat meningkatkan risiko pencurian dan kebocoran data, menyoroti pentingnya keamanan data, termasuk kerahasiaan dan privasi, terutama saat data dibagikan secara jarak jauh. Kriptografi menjadi solusi tepat untuk meningkatkan perlindungan dokumen, menjamin kerahasiaan dan integritas data. Penelitian ini bertujuan untuk mengembangkan sistem keamanan dokumen berbasis website yang mengimplementasikan algoritma vigenere cipher, yang dikenal sebagai sandi substitusi polialfabetik yang kuat terhadap analisis frekuensi. Metode pengembangan yang digunakan adalah waterfall, meliputi analisis, perancangan, implementasi, dan pengujian. Sistem ini dirancang untuk memfasilitasi enkripsi dan dekripsi teks serta gambar, mendukung file berekstensi .txt, .pdf, .png, dan .jpg. Dua komponen utama sistem adalah antarmuka pengguna (frontend) dan logika pemrosesan algoritma (backend). Implementasi dilakukan menggunakan Microsoft Visual Studio Code dengan bahasa pemrograman PHP dan CSS. Hasil pengujian black-box menunjukkan bahwa seluruh fitur sistem, termasuk login, registrasi, enkripsi, dekripsi, dan pengunduhan file terenkripsi/terdekripsi, berfungsi dengan baik sesuai fungsinya. Proses enkripsi berhasil mengubah file dan gambar menjadi susunan karakter acak yang tidak dapat dipahami tanpa kunci khusus, sementara dekripsi mampu mengembalikan file ke bentuk semula menggunakan kunci yang sama. Algoritma vigenere cipher memberikan enkripsi dan dekripsi yang kuat dengan kunci yang sulit diretas, menjaga kerahasiaan data selama proses komunikasi. Secara keseluruhan, sistem keamanan dokumen berbasis website ini terbukti efektif dan layak digunakan untuk meningkatkan keamanan dokumen teks dan gambar, melindungi data sensitif dari akses tidak sah. Keberhasilan implementasi dan pengujian menegaskan kontribusinya dalam konteks perlindungan data sederhana.

Kata kunci: Kriptografi, Algoritma Vigenere Cipher, Enkripsi, Dekripsi.

ABSTRACT

The rapid development of information technology increases the risk of data theft and leakage, highlighting the importance of data security, including privacy and privacy, especially when data is shared remotely. Cryptography is the right solution to improve document protection, ensure data confidentiality and integrity. This study aims to develop a website-based document security system that implements the vigenere cipher algorithm, known as a polyalphabetic substitution cipher that is strong against frequency analysis. The development method used is waterfall, including analysis, design, implementation, and testing. This system is designed to facilitate encryption and decryption of text and images, supporting files with extensions .txt, .pdf, .png, and .jpg. The two main components of the system are the user interface (frontend) and the algorithm processing logic (backend). The implementation is carried out using Microsoft Visual Studio Code with the PHP and CSS programming languages. The results of black-box testing show that all system features, including login, registration, encryption, decryption, and downloading encrypted/decrypted files, function properly according to their functions. The encryption process completes the transformation of files and images into a random sequence of characters that cannot be understood without a special key, while decryption is able to restore the file to its original form using the same key. The Vigenere cipher algorithm provides strong encryption and decryption with a key that is difficult to crack, maintaining data confidentiality during the communication process. Overall, this website-based document security system has proven to be effective and feasible to use to improve the security of text documents and images, protecting sensitive data from unauthorized access. The successful implementation and testing confirm its contribution in the context of simple data protection.

Keywords: Cryptography, Vigenere Cipher Algorithm, Encryption, Decryption.