

ABSTRAK

IMPLEMENTASI ALGORITMA *BLOWFISH* UNTUK PENGAMANAN TRANSAKSI DALAM APLIKASI BERBASIS WEBSITE

Nama : Renki Gunawan
Nim : 6404211079
Dosen Pembimbing : Elvi Rahmi, S.T., M.Kom

Abstrak

Keamanan data transaksi merupakan elemen penting dalam transaksi bisnis di *e-commerce*, terutama di era digital. Penelitian ini bertujuan untuk mengimplementasikan algoritma Blowfish pada aplikasi berbasis web guna meningkatkan keamanan data transaksi dalam sistem *e-commerce* di toko Tri Jaya Bengkalis. Algoritma *Blowfish* dipilih karena efisiensinya dalam enkripsi data dengan struktur *Feistel* dan panjang kunci yang *fleksibel* antara 32 hingga 448 bit, menjadikannya andal dalam menghadapi ancaman keamanan. Sistem ini dirancang untuk mendukung transaksi *e-commerce* dengan menyediakan aplikasi web penjualan *e-commerce* yang aman dan andal. Teknologi *OpenSSL* diterapkan untuk membantu proses enkripsi data, sementara struktur *dictionary attack* digunakan untuk meningkatkan efisiensi pengelolaan kunci enkripsi. Data transaksi, seperti informasi pelanggan dan pembayaran, disimpan dalam bentuk ciphertext di database untuk memastikan perlindungan terhadap akses tidak sah dan manipulasi. Hasil implementasi menunjukkan bahwa algoritma *Blowfish* yang dikombinasikan dengan *OpenSSL* dan *dictionary attack* dapat meningkatkan integritas dan kerahasiaan data transaksi, serta membangun kepercayaan pelanggan terhadap layanan toko.

Kata Kunci : Keamanan Data Transaksi, Algoritma *Blowfish*, Aplikasi Berbasis Web, *Dictionary attack*, *OpenSSL*

ABSTRACT

IMPLEMENTASI ALGORITMA *BLOWFISH* UNTUK PENGAMANAN TRANSAKSI DALAM APLIKASI BERBASIS WEBSITE

Nama : Renki Gunawan
Nim : 6404211079
Dosen Pembimbing : Elvi Rahmi, S.T., M.Kom

Abstract

Transaction data security is an important element in business transactions in e-commerce, especially in the digital era. This research aims to implement the Blowfish algorithm in a web-based application to increase the security of transaction data in the e-commerce system at the Tri Jaya Bengkalis store. The Blowfish algorithm was chosen because of its efficiency in data encryption with a Feistel structure and flexible key length between 32 to 448 bits, making it reliable in dealing with security threats. This system is designed to support e-commerce transactions by providing a secure and reliable e-commerce sales web application. OpenSSL technology is applied to assist the data encryption process, while a dictionary attack structure is used to increase the efficiency of encryption key management. Transaction data, such as customer and payment information, is stored in ciphertext form in the database to ensure protection against unauthorized access and manipulation. The implementation results show that the Blowfish algorithm combined with OpenSSL and dictionary attacks can increase the integrity and confidentiality of transaction data, as well as build customer trust in store services.

Keywords : *E-commerce* Transaction Data Security, *Blowfish* Algorithm, *Ecommerce* Sales Web-Based Application, *Dictionary*, *OpenSSL*.