



INTISARI

RANCANG BANGUN *CRYPTOSYSTEM* UNTUK KEAMANAN FILE PHP MENGUNAKAN ALGORITMA BLOWFISH

Oleh

Kharisma

11/322436/PPA/03558

Permintaan pengembangan aplikasi berbasis website meningkat cukup signifikan. Bagi pengembang aplikasi berbasis website merupakan kesempatan yang baik untuk lebih banyak berkarya, akan tetapi menjadi sebuah dilema ketika akan mendistribusikan aplikasi dengan *source code* yang mudah dibaca dan dibajak, disisi lain pengembang tidak ingin memberikan *source code* kepada semua kliennya.

Penelitian ini berfokus pada membangun sebuah *cryptosystem* menggunakan algoritma blowfish serta membuat sebuah ekstensi PHP dalam rangka untuk mengamankan *source code* PHP agar tidak dapat dibaca oleh orang yang tidak berhak. *Cryptosystem* akan melakukan proses enkripsi file PHP menggunakan kunci yang dinamis sepanjang 128 bit. Hasil enkripsi kemudian ditempatkan pada *web server* yang sudah terpasangkan *PHP Extension* yang telah dipersiapkan terlebih dahulu untuk melakukan dekripsi file PHP secara *on the fly*.

Cryptosystem menggunakan algoritma blowfish dapat mengamankan file PHP terhadap pihak yang tidak berkepentingan. File PHP yang telah terenkripsi dapat dijalankan secara langsung tanpa melakukan dekripsi ke dalam sebuah file terlebih dahulu. File PHP yang asli dan file yang telah terenkripsi tidak mengalami perubahan waktu eksekusi yang cukup signifikan.

Kata kunci : *source code*, PHP, *cryptosystem*, *PHP extension*, algoritma blowfish.



ABSTRACT

DESIGN OF CRYPTOSYSTEM FOR THE SECURITY OF PHP FILE USING THE BLOWFISH ALGORITHM

By

Kharisma

11/322436/PPA/03558

Demand of web-based application development increased significantly. For web-based application developers this is a good opportunity for more valuable work, but becomes a dilemma when it will distribute applications with source code that is easy to read and hijacked, on the other hand the developer does not want to provide source code to all of their clients.

This study focuses on building a cryptosystem using blowfish algorithm and create a PHP extension in order to secure the PHP source code that can not be read by unauthorized people. Cryptosystem will perform the encryption process PHP files using dynamic keys along the 128 bit. Result of the encryption file is then placed on a web server that already installed PHP extension that has been prepared in advance to decrypt the PHP files on the fly.

Cryptosystem using blowfish algorithm can secure PHP files against unauthorized access. PHP files that have been encrypted can be run directly without decryption into a file beforehand. The original PHP files and encrypted files have not changes significantly related to the execution time.

Keyword: source code, PHP, cryptosystem, php extension, blowfish algorithm.