Abstrak

Tujuan sistem manajemen pembelajaran adalah untuk membantu kegiatan belajar. Sistem membantu mengelola tugas, proses penilaian, dan komunikasi pengguna. Untuk menghindari akses data yang ti dak sah, sistem manajemen pembelajaran membutuhkan mekanisme untuk melindungi password yang digunakan dalam proses login sistem. Enkripsi database menggunakan algoritma Rijndael diusulkan oleh Francis Onodueze dkk. untuk melindungi data. Sebuah kunci diperlukan untuk proses enkripsi, dan kunci tersebut harus tetap rahasia. Jadi, ketika kuncinya statis, ia rentan terhadap serangan menebak kunci. Un tuk mengatasi kelemahan kunci statis, diusulkan pembuatan kunci dinamis menggunakan Hash Messages Authentication Code - Deterministic Random Bit Generator (HMAC-DRBG) karena dapat menghasilkan kunci secara berkala. Berdasarkan hasil evaluasi, peluang sukses terhadap penyerangan penebakan kunci dari metode yang diusulkan lebih kecil dibandingkan dengan metode yang diusulkan sebelumnya, dimana kompleksitas waktu yang dibutuhkan oleh kedua metode sama.

Kata kunci : Rijndael, HMAC-DRBG, Pseudorandom-bit.