Abstract

The course management system’s goal is to help learning activities. The system helps to manage tasks, the grading process, and user communications. To avoid unauthorized data access, the course management system needs a mechanism to protect the password that is used in the system’s login process. Database encryption using Rijndael algorithm is proposed by Francis Onodueze et al. to protect the data. A key is needed for the encryption process, and the key has to be kept secret. Thus, when the key is static, it is vulnerable against key guessing attacks. To overcome the static key’s drawback, a dynamic key generation using Hash Messages Authentication Code - Deterministic Random Bit Generator (HMAC-DRBG) is proposed because it can generate keys periodically. Based on the evaluation, the probability of success key guessing attack using the proposed method is less than using the previous method, while the time complexity of those methods is similar.

Keywords: Rijndael, HMAC-DRBG, Pseudorandom-bit.