1. Pendahuluan

Latar Belakang

Sistem manajemen pembelajaran berfungsi untuk mempermudah kegiatan belajar mengajar. Sistem ini membantu dalam mengelola tugas, penilaian, dan komunikasi antar pengguna. Untuk dapat mengakses sistem tersebut, pengguna harus melakukan registrasi dan login, di mana pengguna harus memasukan data seperti username dan password. Karena kombinasi username dan password merupakan identitas unik yang membuat pengguna dapat mengakses *content* yang terdapat dalam sistem manajemen pembelajaran, maka password perlu dilindungi untuk menghindari akses data oleh pihak-pihak yang tidak berwenang.

Berdasarkan alasan yang telah disebutkan sebelumnya dibutuhkan sebuah mekanisme yang dapat mengamankan data kombinasi username dan password pada database sistem manajemen pembelajaran. Salah satu diantaranya adalah metode enkripsi database level kolom yang diusulkan oleh Francis Onodueze [1]. Francise Onodueze, dkk mengusulkan metode enkripsi database level kolom dengan menggunakan algoritma Rijndael, yang memerlukan kunci sebagai bagian penting pada proses enkripsi. Konsep enkripsi yang diusulkan [1] memiliki kelemahan berupa penggunaan kunci yang masih statis (tidak pernah berubah). Hal ini mengakibatkan adanya kerentanan terhadap serangan penebakan kunci.

Topik dan Batasannya

Berdasarkan latar belakang yang telah disebutkan sebelumnya, diperoleh rumusan masalah dari metode yang diusulkan oleh Francis Onodueze, dkk. [1], yaitu bahwa kunci yang digunakan pada proses enkripsi masih rentan terhadap penyerangan penebakan kunci. Kerentanan ini disebabkan karena kunci yang bersifat statis.

Batasan dari penelitian ini adalah kunci dinamis ini akan dimanfaatkan untuk mengamankan akses terhadap data yang berkaitan dengan sistem manajemen pembelajaran pada proses registrasi dan login.

Tujuan

Tujuan dari penelitian ini adalah untuk mengamankan password pada database sistem manajemen pembelajaran pada level kolom menggunakan kunci yang dinamis. Kunci dinamis ini dibangkitkan dengan menggunakan HMAC-DRBG. Pemilihan HMAC-DRBG didasari oleh kemampuan dari metode tersebut, yaitu dapat membangkitkan bilangan acak secara periodik [2]. Bilangan acak tersebut dijadikan sebagai kunci. Dengan demikian kunci yang dihasilkan akan bersifat dinamis.