ABSTRAK

Aplikasi chat berberbasis web saat ini cukup banyak namun fitur keamanan yang diterapkan masih kurang maksimal. Faktanya penerapan algoritma MD5 pada autentikasi login juga rentan terhadap serangan *rainbow table*. Saat ini diketahui sudah ada beberapa metode yang dapat digunakan untuk meningkatkan pengamanan tersebut diantaranya menggunakan *Hypertext Transfer Protocol Secure* (HTTPS) dan *Completely Automated Public Turing Test to Tell Computer and Human Apart* (CAPTCHA). Namun beberapa hasil penelitian terkait memperlihatkan masih terdapat beberapa keamanan dan penggunaan HTTPS, dan CAPTCHA. Penelitian ini mengusulkan penggunaan *Algoritma Advanced Encyrption Standard* (AES) sebagai autentikasi key pada saat user melakukan login untuk meningkatkan keamanan pada aplikasi chatting. Hasil penelitian menunjukan penerapan algoritma MD5 dan AES dapat mengamankan proses autentikasi data user dari serangan *rainbow table*.

Kata Kunci : *Autentikasi Key, Chatting, AES 256 bit, Website*