IMPLEMENTATION OF THE ENCRYPTION SYSTEM USING THE AES CRYPTOGRAPHY METHOD IN THE COUNSELING CHAT APPLICATION

(Case Study: SMKN 1 Ngawi)

MOGAR NURHANDHI
Informatics Study Program, Faculty of Science & Technology
University of Technology Yogyakarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail : mogarnurhandhi@gmail.com

ABSTRACT

The activities of using the internet and exchanging information as well as sending messages have widely used internet media, one of which is chat messaging media, but as time goes by, the problem of security of messages and information in email messages that is often encountered is active or passive eavesdropping. In this final research assignment, the author wants to create a counseling chat message security application using the AES (Advanced Encryption Standard) algorithm cryptographic method. By combining the ECB (Electronic Code Book) technique and the next generation, namely CBC (Cipher Block Chaining). AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Based on a fixed block size, AES works on a 4x4 matrix where each matrix cell consists of 1 byte (8 bits). Based on these problems, research will be carried out to create an application that aims to accommodate the counseling process. The focus of this research is divided into two, namely securing messages with text data type using ECB mode and stored in a database service (Backend as a Service). Then secure messages with image data type using CBC mode and also stored in a database service (Backend as a Service). As well as using the End-to-End service principle so that users do not need to carry out the encryption or decryption process directly because the process has already been carried out by the system, this will also provide more security aspects in terms of confidentiality of key data and initialization vectors. So that the process of exchanging information using the counseling chat application media is secure and protected from eavesdropping by irresponsible parties.

Keywords: Cryptography, Encryption, Chat Messages, Advanced Encryption Standard.