# *IMPLEMENTATION OF AES-128 AND RC6 CRYPTOGRAPHY ALGORITHM FOR WEB-BASED EMAIL ENCRYPTION AND DESCRIPTION*

**TOPAN**
*Informatics Study Program, Faculty of Science & Technology*
*University of Technology Yogyakarta*
*Jl. Ringroad Utara Jombor Sleman Yogyakarta*
*E-mail : topanxtm3kuningan@gmail.com*

## *ABSTRACT*

*Internet user activity continues to increase, reaching 215.6 million people in Indonesia based on a survey by the Indonesian Internet Service Providers Association in 2023, with growth of 1.17% from the previous year. Information technology facilitates the exchange of information via the internet, enabling communication without the limitations of distance and time. However, data security is crucial to protect important information. Email, as a means of exchanging information, faces security challenges such as passive and active eavesdropping. Passive eavesdropping occurs because most emails are transmitted without encryption, allowing people to view or intercept the contents of the email via data traffic. While active interception involves modifying the contents of emails during transportation or storage. To overcome this problem, the author aims to create an email security system by changing email messages (plaintext) into messages that are not easy to read (ciphertext) using cryptographic techniques with the Advanced Encryption Standard (AES-128 byte) and Rivest Cipher 6 (RC6) algorithms. ), two methods that have been tested for security by the National Institute of Standards and Technology (NIST). The results of this research produce email messages that are encrypted during the sending process, so that emails are sent via data traffic and when received are in ciphertext form.*

*Keywords: Data security, Email, Cryptography, Advanced Encryption Standard and Rivest Cipher 6.*