**Abstract**

**Student identification cards (KTM) are currently vulnerable to fraudulent activities and counterfeiting, including replay attacks. KTMs have several functions, such as providing access to parking areas, lecture buildings, libraries, and student attendance systems. Replay attacks allow attackers to falsify student attendance and gain unauthorized access to campus facilities. Therefore, the main objective of this Final Project is to enhance the security of KTMs by implementing a security system based on Advanced Encryption Standard (AES) and rolling code to prevent replay attacks. The method used involves encrypting data on KTMs using the AES-128 algorithm and applying rolling code in the KTM security system. The test results show that the implementation of a security system based on AES-128 encryption and rolling code on KTMs can enhance the security and authenticity of KTMs and prevent fraudulent activities and counterfeiting, including card duplication. Thus, this Final Project provides a solution to improve KTM security and offers significant benefits for KTM users.**

**Keywords: Replay Attack, Radio Frequency Identification, Advanced Encryption Standard, Near Field Communication, Rolling code.**