CHAPTER 1
INTRODUCTION

1.1. Background

The Radio Frequency Identification Technology (RFID) was invented during the war to identify whether the planes belong to fellow British soldiers or an enemy of the British army during World War II [1]. Nowadays, RFID has come along the way to mainstream commercial usage accompanied by an advance in technology. Nevertheless, along with easy access to RFID technology today, security concerns have increased from past years. People could quickly build an RFID reader with minimal cost and read RFID tags to extract data inside the chip. For example, someone could copy and clone the data inside an RFID chip using a handmade RFID reader and use it to unlock an unsecured RFID implemented door or gate using RFID using cloned RFID tags. This scenario will create a new problem when the data inside the chip is essential, valuable information of the said victim.

To secure the data inside the RFID chip when someone unauthorized tries to access, read, or clone the RFID tags. A lightweight encryption algorithm implemented that will not burden the Arduino controller when running the said algorithm program. Another factor besides that, a compression algorithm will be implemented before encryption to help reduce data redundancy and decrease the time of encryption of data. There are two types of encryption algorithm based on the key used to encrypt and decrypt the data. This project will compare the two algorithms to which one of the algorithms is more efficient for the Arduino UNO controller. The asymmetric cryptography representation is the RSA (Rivest-Shamir-Adleman) encryption algorithm and the symmetric cryptography representation is the AES (Advanced Encryption Standard) encryption algorithm. Those algorithms are chosen because these two are commonly used and still relevant to this day. Furthermore, implementing a simple compression method based on the Huffman encoding algorithm supports fast and efficient RFID data security measures.

The project was carried using encryption from the RSA algorithm and AES algorithm. The algorithms are tested in combination with compression and without compression to know which combination is better suited. The method using AES encryption is the fastest to complete encryption and decryption. However, the combination of encryption and compression is the

safest and could reduce data redundancy inside small RFID tags memory, which is only 16 bytes of data per block.

1.2. Problem Formulation

1. Which is the faster RSA or AES algorithm on the Arduino controller?
2. How effective is simple compression using encoding based on the Huffman algorithm?
3. What is the best combination of RFID securing methods?

1.3. Scope

1. Implement RSA and AES encryption algorithm on Arduino controller.
2. Implement a simple Huffman encoding algorithm.
3. Compare the combination of algorithms in terms of the speed of encryption and decryption process.

1.4. Objective

This research aims to implement symmetric and asymmetric algorithms that are fast and secure for RFID tag data between RSA and AES cryptographic algorithms—at the same time, testing the implementation compression as a supporting algorithm to reduce data redundancy in RFID tags memory block.