CHAPTER 1
INTRODUCTION

1.1 Background

Nowadays, telemedicine is commonly used to diagnose patients from a long distance. Telemedicine is the use of information and communication technology combined with medical expertise to provide health services, ranging from consultation, diagnosis and medical treatment, without limited space or carried out remotely (Jamil, Khairan, & Fuad, 2015). Many doctors and medical personnel have entrusted the use of telemedicine because it is efficient for remote health control and many of the tools used are based on the embedded system. In the implementation, one of the challenges faced in telemedicine today is security. Encryption is needed when sending data, so the data cannot be changed, read, opened, or accessed by unauthorized people.

To keep the data sent by embedded systems unchanged, can't be read, opened, or accessed by unauthorized people, a lightweight encryption algorithm is needed, so the Arduino easily to executing programs. Besides being lightweight, a fast algorithm is needed and uses less power because examination equipment allows using batteries. Based on the type of key used, there are two types of encryption or cryptographic algorithms namely symmetric cryptography and asymmetric cryptography. To send and receive light data in this project, the algorithm that is suitable for use is a symmetrical cryptographic algorithm. In symmetric cryptography, the process of encryption and decryption use the same key, so the process is relatively fast. This is caused by the efficiency that occurs in the key generator. The popular or widely used symmetrical cryptographic algorithms are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES).

In this project, research was carried out on the DES and AES algorithms. From the comparison of the two algorithms tested, the algorithm that has the fastest / most efficient encryption process and uses less power is used to create a telemedicine system. In addition, the compatibility of encryption in Arduino will also be tested and decrypt in Php.

1.2 Scope

1. Implement DES and AES on Arduino
2. Comparing DES and AES in terms of the speed of the encryption process and the power consumption

1.3 Objective

The purpose of this project is to implement and compare cryptographic algorithms that are fast, lightweight and use less power between DES and AES symmetrical cryptographic algorithms. The right algorithm will be used to create a system for sending heart rate data, patient body temperature, or others in telemedicine. The doctor's diagnosis can be done easily and accurately even for patients who are far away.