ABSTRACT

Along with the times, the field of Internet of Things (IoT) technology is increasingly advanced, especially in the field of data transmission and storage. But who would have guessed that it turned out that behind the rapid technological advances harbored a fear of data theft. As for the solution to overcome data theft, the system should use Cryptography. Cryptography can minimize data theft so that it is not misused. In this final project research, a system will be designed that can maintain security in the process of sending data IoT through the MQTT protocol of data storage on PHP MyAdmin with the RSA Method.

The sensor data used uses the ultrasonic sensor HC-SR04 which is applied in the Raspberry Pi 4 microcomputer. Sensor data entering the system is automatically converted into chipertext using the RSA method with two scenarios, namely 1024 bit and 2048 bit RSA. After that, the data will be sent via MQTT to the PHP Myadmin database. In the data database in the form of chipertext, it will automatically be decrypted.

Based on the test results of the system, it is known that the system can encrypt sensor data and can transmit data in the form of chipertext through MQTT to the database. The average response times value for a 1024 bit RSA scenario was 879.4 ms for the encryption process and 2189.83 ms for the decryption process. For the 2048 bit RSA scenario, the average Response Times test results for 10, 20, and 30 data were 2,859.27 ms for the encryption process and 228,060.91 ms for the decryption process. The process of sending data from the sensor to the database shows that the QoS on the system that has been created is included in the excellent category with values for the RSA scenario of 1024 bit and RSA 2048 bit, namely throughput of 6932.04 Kb/s and 6167.03 Kb/s, packet loss of 0% and delay of 243.3 ms and 589.5 ms.

Keywords *: RSA, Internet of Things, Security System, Encryption, Decryption, MQTT.*