CHAPTER 6
CONCLUSION

This study concludes that AES and RSA encryption can be implemented on Arduino UNO using the Arduino software to program the system.

For the encryption process the test result has shown that AES, on average, is 145768 microseconds faster than RSA in encryption without compression. Also, when tested with compression, AES is 134193.45 microseconds faster than RSA. Note that these tests are using the same length of data.

The compression using RLE or Run-Length Encoding is only effective when the data input is repeated in alphabetical characters. When tested using this method, RLE could compress manual input text with the length of the character of 16 are between 12.5% to 50% efficiency. RLE also improved the encryption time of the RSA algorithm by up to 6.39%.

This research concludes that the AES as encryption alone is more time-efficient and safer than RSA because AES shifts each of the characters multiple times compared to RSA one time only. However, for the compression combined with encryption, the RSA is more suitable to be combined with Run Length Encoding. The RSA does not need any padding character for the encryption to work correctly, but it comes with a sacrifice in computation time.

Suggestion for future study on this research to plaintext for AES to be more flexible, there is no need for padding anymore for it to work correctly if the input is lower than 16 characters. The RSA could generate its key automatically. Furthermore, the compression method is not only limited to repeated characters.