International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Implementation of AES Algorithm in Arduino Mega2560 board

Hemala Nallamuthu

M.E. scholar, Dept. of Electronics and Communication Engineering, Nandha Engineering College, Tamilnadu, India.

Abstract - *Microcontrollers are utilized worldwide in different electronic items. It utilizes sensors to get acquainted with ecological parameters, or, in other words executing a specific activity. This information, gathered from sensors, are regularly transmitted to the microcontroller either through a wired or remote medium. Along these lines, such information could be read by an unapproved individual, which could be a high risk of utilizing the item. Henceforth, a security protocol must be received with the end goal to guarantee the safe transmission of information through any terminal. AES is the advanced encryption standard that is utilized with the end goal to give a high security to the information being transmitted. In this paper, a straightforward variant of AES algorithms is implemented in Arduino Mega2560 board, with an aim to guarantee the protected transmission of information. This could be additionally enhanced by changing key sizes, expanding or diminishing rounds of encryption and so forth.*

***Key Words*: AES, Arduino, Cryptography, DES, Encryption.**

1. INTRODUCTION

Internet of Things [1] is changing the world. Technology together with innovation is changing every bit of day to day life. From home to industries, Smartphones, smart gadgets and sensors gather information to facilitate people. Consequently, every information is made accessible to the installed embedded frameworks around us. In the event that any unapproved individual gains admittance to this information, it would result in exceptional impacts. Subsequently, it is very basic to keep our information anchored from assailants.

Cryptography [2] is the field of study, which involves different schemes utilized for anchoring information. It incorporates encryption strategies, which changes over the plaintext (message to be anchored) into cipher content (encoded message) with the assistance of key. Substitution and transposition are the two essential building blocks of encryption. In substitution, either letter of the plaintext is replaced by different letters or numbers or images or bit pattern of plaintext is replaced by the bit pattern of ciphertext.

The approved individual could undoubtedly decode the scrambled message with the assistance of keys. At the point when both encryption and decryption utilizes a similar key, it is called symmetric encryption. On the off chance that diverse keys are utilized, it is called decryption. In this paper, simple version AES algorithm is implemented on Arduino Mega2560 board. Along these lines, cryptography is utilized to take care of information leakage issues in present-day installed frameworks.

2. RELATED WORKS

DES – Data Encryption Standard [3] has been embraced by NIST in 1977 as the official encryption algorithm. It utilizes 56-bit key and 16 rounds of encryption including different stages, for example, permutation, substitution, and transposition. These methods are utilized to create ciphertext from plaintext. In the Brute-force assault, for 56 bit key 256 key blends are should have been tried with the end goal to locate the correct key, which was inconceivable when 1977. With ongoing progression in technologies and creation of multicore processors, DES algorithm was broken down in few minutes with different strategies.

Conquering the disadvantage of lessened key size in DES, 3DES (Triple DES)[4] standard has been proposed and adopted. It utilizes indistinguishable algorithm from DES with an enhanced key size of around 168 bits long. Its key size is 3 times that of DES algorithm i.e., 56*3 = 168-bit key and 16*3 = 48 rounds of encryption is adopted. Consequently, 2^{168} key mixes are accessible, which is far separated for the Brute-force attack. Consequently, 3DES has been received as the proficient algorithm.

From a relative study[5], it very well may be presumed that the AES – Advanced Encryption Algorithm turns out to be the most proficient and propelled algorithm, superior to that of DES, 3DES and RSA algorithms. It utilizes three diverse key sizes of 128, 192 and 256 bits wide with enhanced security including distinctive rounds of encryption – 10, 12 and 14 rounds respectively. Subsequently, in this paper AES algorithm is picked and implemented on the Arduino Mega2560 board.

3. ADVANCED ENCRYPTION STANDARD

AES is a symmetric block cipher, which operates on 128 bit block of key and input. Same key is used for both encryption and decryption of AES process. Keys used in this algorithm is available in three variants, i.e., 128, 196 and 256 bits. Out of these keys, 128 bit key is the most widely used one. Other two keys also offers an enhanced security. Key parameters of AES process[2] is shown in the table 1.

Table- 1: AES Parameters

Key size (words /bytes/bit)	4/16/128	6/24/192	8/32/256
Plaintext block size	4/16/128	4/16/128	4/16/128

(words /bytes/bits)			
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size(words /bytes)	44/176	52/208	60/240

Encryption and Decryption process of AES can be demonstrated as follows:

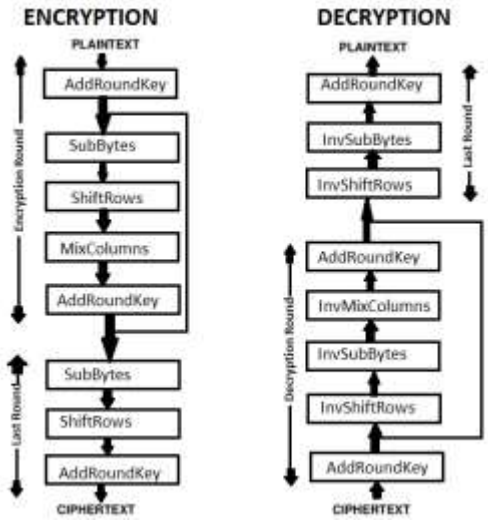

Fig-1: AES Encryption and Decryption Process

Diverse kinds of assaults are endeavored to break AES calculations like square attack, key attack, and differential attack. Be that as it may, none of them has broken the calculation. Henceforth, AES is viewed as the most secure one.

Following are the rounds involved in encryption process:

3.1 Substitution bytes: Obtained input message is changed over into hexadecimal esteem, whose every 4-byte component is utilized as the row and column estimation of Sbox. In this way, every component relates to a one of a kind component from Sbox.

3.2 Shift Rows: Here, the bytes of the last three rows are circularly shifted. The second column includes 1 byte left circular shift. Though third and fourth rows include 2 and 3 bytes left round shift separately.

3.3 Mixcolumns: It changes every section into another segment to deliver expanded disarray and dissemination.

3.4 Addroundkey: The Key network is XORed with the information lattice to deliver another arrangement of information.

4. RESULT:

Encryption time and memory utilization are the two parameters involved in deciding the most suited encryption algorithm for resource constrained devices. AES algorithm is thus coded in Arduino programming language, compiled and uploaded to Arduino mega board. Following output is obtained. Output is shown in figure 2 and 3.

4.1 Memory usage of code from Arduino IDE:

From Arduino IDE,
Sketch uses 8824 bytes (3%) of program storage space. Maximum is 253952 bytes.
Global variables use 800 bytes (9%) of dynamic memory, leaving 7392 bytes for local variables. Maximum is 8192 bytes.

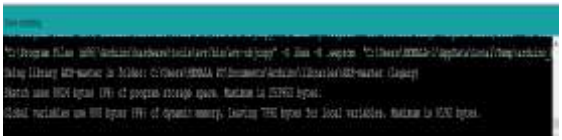

Figure 2 Memory usage of AES code involved.

4.2 Encryption time:

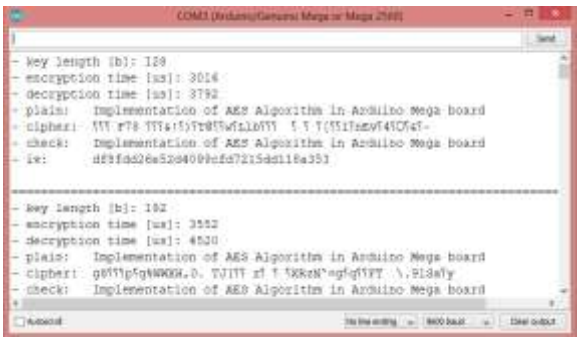

Figure 3 Output of AES process from Arduino Mega board

From output, time taken for encryption is 3016 µs and for decryption is 3792 µs.

5.CONCLUSION:

The use of internet is growing rapidly. Usage of security algorithms ensures the security of our information. Thus, in this paper, AES encryption process is implemented in Arduino mega2560 board, which proves to be the efficient algorithm that can be implemented for resource constrained devices.

REFERENCES

[1] Ashvini Kamble, Sonali Bhutad, "Survey On Internet Of Things (Iot) - Security Issues & Solution" in proceedings of the second International Conference on Inventive Systems and Control (ICISC 2018).

[2] "Cryptography and Network Security, Principles and Practices", Fourth Edition by William Stallings.

[3] Mukta Sharma, Dr. R.B. Garg,"DES: The Oldest Symmetric Block Key Encryption Algorithm", in the proceedings of the SMART -2016, IEEE Conference ID: 39669 5th International Conference on System Modeling & Advancement in Research Trends, 25th – 27th November, 2016.

[4] Karthik .S, Muruganandam.A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System", International Journal of Scientific Engineering and Research (IJSER) Volume 2 Issue 11, November 2014.

[5] R. Sivakumar, B. Balakumar, V. Arivu Pandeeswaran, "A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security", International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 04 Apr-2018.