ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

# AES Based Cryptography System for Secured Communication

V.V.Valli Kanakadurga[1] , P.V.V.N.D.P.Sunil[2] , T.Harika[3] , Naheed Sulthana[4] , T.Maheshbabu[5] ,

B.Tech, Dept. of ECE, D.M.S.S.V.H College of Engineering, Machilipatnam, India[1345] .

Assistant Professor, Dept. of ECE, D.M.S.S.V.H College of Engineering, Machilipatnam, India[2] .

**ABSTRACT**: The objective of the project is to design a “AES based Cryptography system for secured communication”. Security in digital transmission is an increasingly interesting topic in a number of fields. Security plays key role in the exchange of messages between different sites of military and/or other critical organizations that are concerned about information security. Therefore encrypting the information before transmission and decryption to retrieve the information is important. AES Cryptography is a well-known example of public key cryptographic algorithms that involves robust encryption/decryption processes. On the other hand self controlled embedded systems deployed in various fields can send crucial information. Single-board computer with wireless LAN connectivity. This smart card sized computer became popular for its computing power and small factor in embedded field. In this project, we try to implement AES encryption algorithm on Raspberry Pi to construct an unique wireless cryptographic system, that would become powerful embedded platform that can be used for secured communication.
There exists a paper in the literature where RSA (Rivest–Shamir–Adleman) algorithm implemented on Raspberry Pi , the RSA is a public-key encryption algorithm (asymmetric), while AES is a symmetric key algorithm. Meaning that the same key is used for both encryption and decryption. AES provides better security too, cracking an AES key with a state-of-the-art supercomputer would take longer than the presumed age of the universe. As of today, no practicable attack against AES exists. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world. We chose AES algorithm because it is faster to be used for embedded platforms like Raspberry Pi. Our demonstration equipment contains two parts, one is the AES encryption algorithm running on Raspberry Pi and the second is the decryption algorithm running on a laptop. A wireless link is established between the Pi and the laptop. We demonstrate the secured communication happening between the laptop and Pi.

**KEYWORDS**: Raspberry Pi 3 Model B, AES, Data Encryption and Decryption, Cryptography, security, Laptop.

## I. INTRODUCTION

In present day scenario, the security of communication is a crucial issue on World Wide Web. Secure communication is when two entities are communicating and do not want a third party to listen in. Data is any type of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, personal databases and websites. Cryptography is evergreen and developments. The advancement of technology is bringing more comforts in to the Hackers to theft the data, these reasons are leading to the increase in number of hackings. Security of information has become a tremendous term for information and communication technology nowadays. Cryptography is a popular ways of sending vital information in a secret way. There are many cryptographic techniques available and among them AES is one of the most powerful techniques. This idea motivated us to introduce a cryptography system for secured communication that will communicate the information with security, which will improve the convenience of the users to secure their communication. In these days Internet world security plays a very important role in securing data. After noticing constant reports of data theft and hacking, enhancing security of the data has become mandatory. We choose ARM Raspberry Pi board as hardware platform for experimental setup. To enable Raspberry Pi system on chip (SoC), inbuilt WIFI and Bluetooth are perform cryptographic computation. This paper deals with information related to cryptography.

DOI: 10.15680/IJIRCCE.2018.0602050

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

**International Journal of Innovative Research in Computer and Communication Engineering**

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

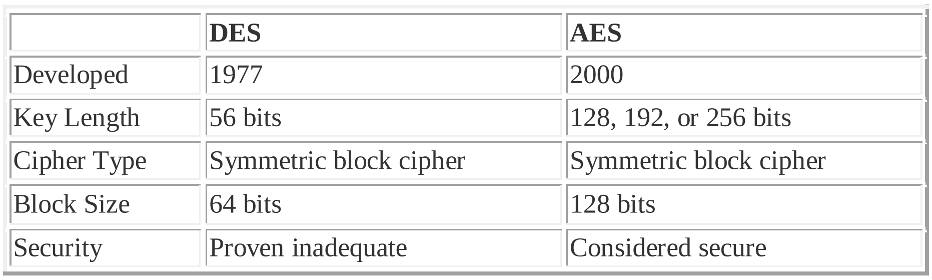
**Vol. 6, Issue 2, February 2018**

## II. MAIN CONCEPT

The main theme of our project is Securing the communication through AES algorithm using cryptography and Raspberry Pi 3 Model B.

## III. RELATED WORK

Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval. Previously we use DES, DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block. The plaintext block has to shift the bits around. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation. But Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure - 2. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.
The main drawback of DES is Comparatively slower, but AES is faster. The reason we will use AES Is shown in given table 1.



| | DES | AES |
|---|---|---|
| Developed | 1977 | 2000 |
| Key Length | 56 bits | 128, 192, or 256 bits |
| Cipher Type | Symmetric block cipher | Symmetric block cipher |
| Block Size | 64 bits | 128 bits |
| Security | Proven inadequate | Considered secure |

Table 1: Difference between AES and DES

## IV. PROPOSED SYSTEM

### A. Block Diagram:

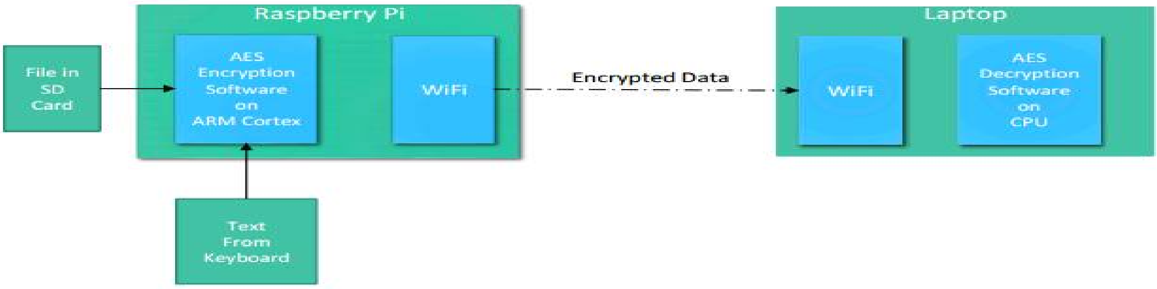


Fig. 1. Block diagram of the system

The block diagram of AES based cryptography system for secured communication is shown in above figure.

B. **Raspberry Pi 3 Model B:**

The Raspberry Pi 3 Model B is the third generation Raspberry Pi. This powerful credit-card sized single board computer can be used for many applications and supersedes the original Raspberry Pi Model B+ and Raspberry Pi 2 Model B. Whilst maintaining the popular board format the Raspberry Pi 3 Model B brings you a more powerful processer, 10x faster than the first generation Raspberry Pi. Additionally it adds wireless LAN & Bluetooth connectivity making it the ideal solution for powerful connected designs.

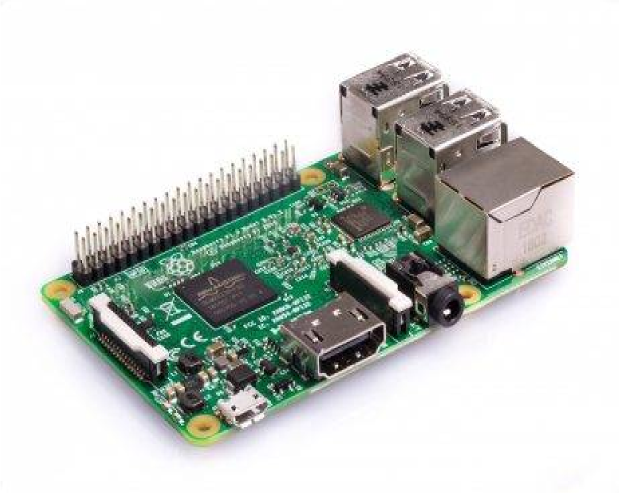
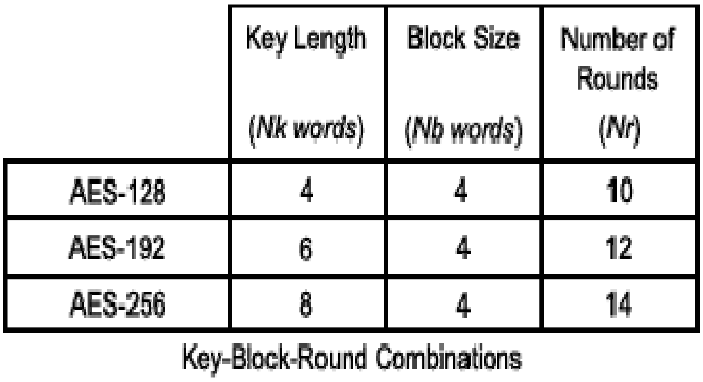


Fig. 2. Raspberry Pi 3 Model B

**C. AES:**

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.



|  | Key Length<br>(*Nk* words) | Block Size<br>(*Nb* words) | Number of Rounds<br>(*Nr*) |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

Key-Block-Round Combinations

Table 2. key-Block-Round Combinations

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm.

The four stages are as follows: 1. Substitute bytes 2. Shift rows 3. Mix Columns 4. Add Round Key

Execute the following operations which are described above. 1. Sub Bytes 2. Shift Rows 3. Add Round Key, using K(10)

Encryption : Each round consists of the following four steps:

i Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii Shift Rows : In the encryption, the transformation is called Shift Rows.

iii Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv Add Round Key : Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the “Mix columns” step.

Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the “Inversemix columns” step

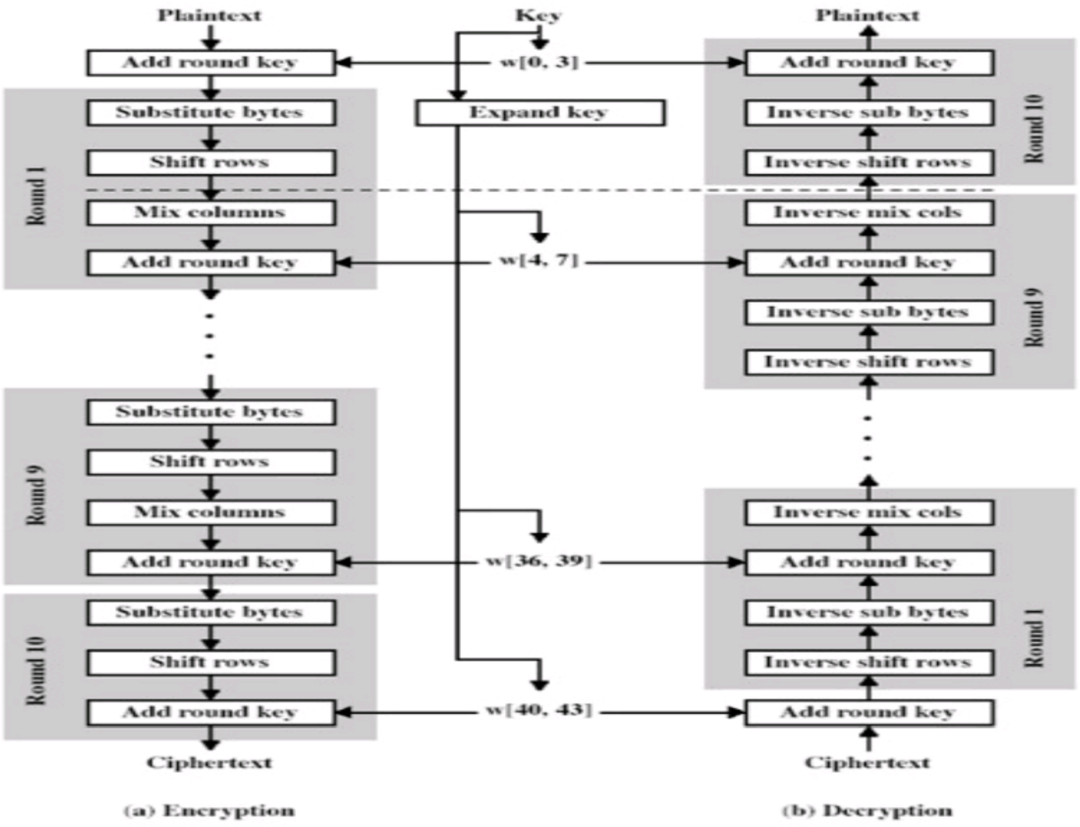
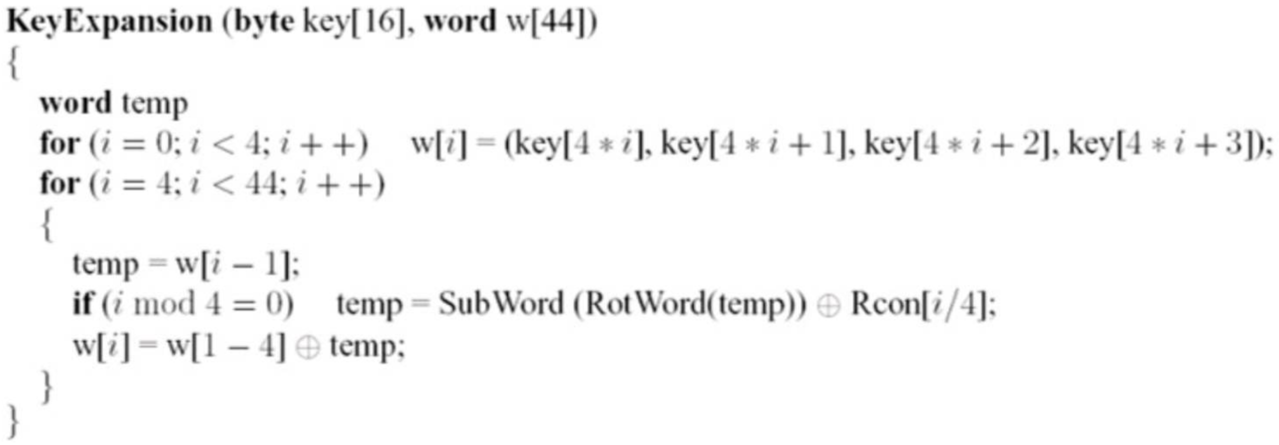


Fig. 3. Overall structure of AES Algorithm



```
KeyExpansion (byte key[16], word w[44])
{
  word temp
  for ($i = 0; i < 4; i++$)    w[$i$] = (key[$4*i$], key[$4*i+1$], key[$4*i+2$], key[$4*i+3$]);
  for ($i = 4; i < 44; i++$)
  {
    temp = w[$i - 1$];
    if ($i$ mod $4 = 0$)    temp = SubWord (RotWord(temp)) $\oplus$ Rcon[$i/4$];
    w[$i$] = w[$1 - 4$] $\oplus$ temp;
  }
}
```

Fig. 4. AES key expansion

The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words. Each round uses 4 of these words. Each word contains 32 bytes which means each sub key is 128 bits long. show pseudo code for generating the expanded key from the actual key .

The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word w[i] depends on the immediately preceding word, w[i − 1], and the word four positions back w[i − 4]. In three out of four cases, a simple XOR is used. For a word whose position in the w array is a multiple of 4, a more complex function is used. The generation of the first eight words of the expanded key using the symbol g to represent that complex function. The function g consists of the following sub functions:

1. Rot Word performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].

2. Sub Word performs a byte substitution on each byte of its input word, using the s-box described earlier.

3. The result of steps 1 and 2 is XORed with round constant, Rcon[j].

The round constant is a word in which the three rightmost bytes are always 0. Thus the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j] = (RC[J], 0,0,0), with RC[1]= 1, RC[j]= 2• RC[j − 1] and with multiplication defined over the field GF($2^8$ ).

The key expansion was designed to be resistant to known cryptanalytic attacks. The inclusion of a round-dependent round constant eliminates the symmetry, or similarity, between the way in which round keys are generated in different rounds.

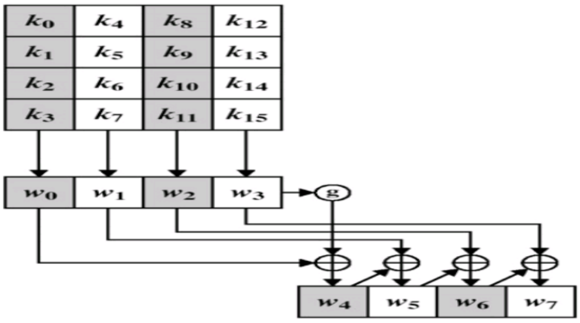


Fig. 5. AES Key Expansion

**CBC Mode**: CBC mode of operation provides message dependence for generating cipher text and makes the system non-deterministic.

**Operation:**
The operation of CBC mode is depicted in the following illustration. The steps are as follows

- Load the n-bit Initialization Vector (IV) in the top register.
- XOR the n-bit plaintext block with data value in top register.
- Encrypt the result of XOR operation with underlying block cipher with key K.
- Feed cipher text block into top register and continue the operation till all plaintext blocks are processed.
- For decryption (IV) data is XORed with first cipher block is decrypted. The first cipher block is also fed into register replacing IV for decrypting next cipher block.

**D. Cryptography:**
The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fuelled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations. The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction.

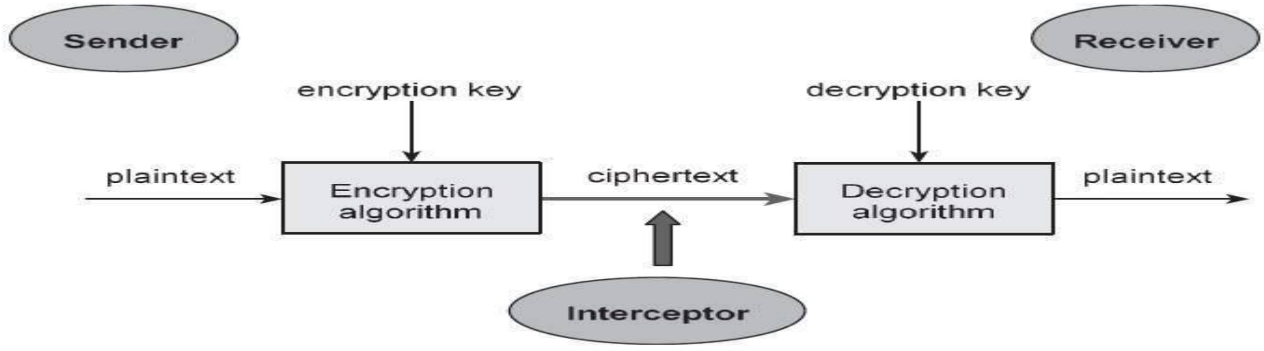


Fig. 6. Cryptosystem

The hiding of information is called encryption, and when the information is unhidden, it is called decryption. A cipher is used to accomplish the encryption and decryption. Merriam-Webster's Collegiate Dictionary defines cipher as a method of transforming a text in order to conceal its meaning. The information that is being hidden is called plaintext; once it has been encrypted, it is called cipher text. To hide any data two techniques are mainly used one is Cryptography other is Steganography. In this paper we use Cryptography. Cryptography is the science of protecting data, which provides methods of converting data into unreadable form, so that Valid User can access Information at the Destination. Cryptography is the science of using mathematics to encrypt and decrypt data.

**Data Encryption**
A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique. Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a

block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time. Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

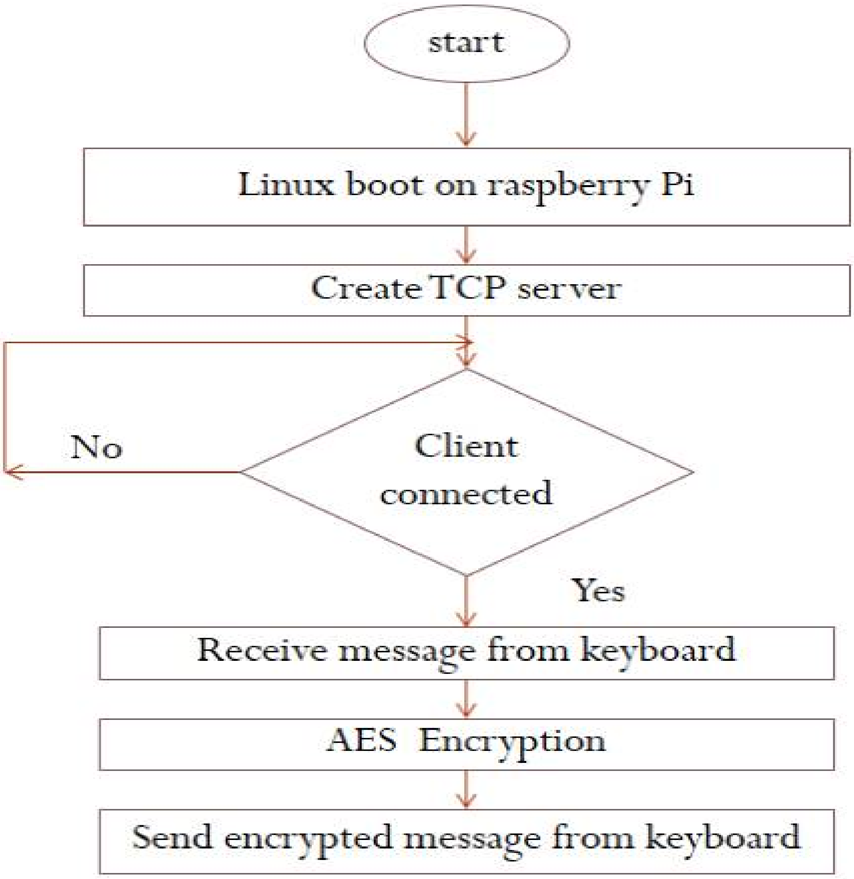

start
Linux boot on raspberry Pi
Create TCP server
No
Client connected
Yes
Receive message from keyboard
AES Encryption
Send encrypted message from keyboard

Fig. 7. Flowchart for Data Encryption

**Data Decryption**

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is the process of converting cipher text back to plaintext.

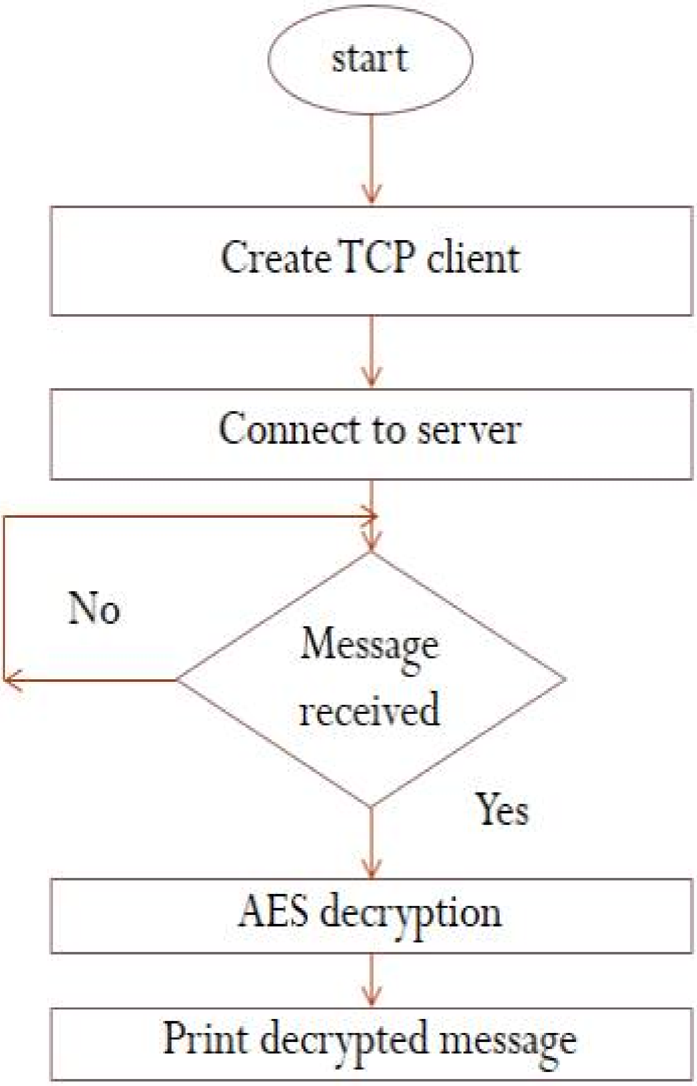


Fig. 8. Flow chart for Data Decryption

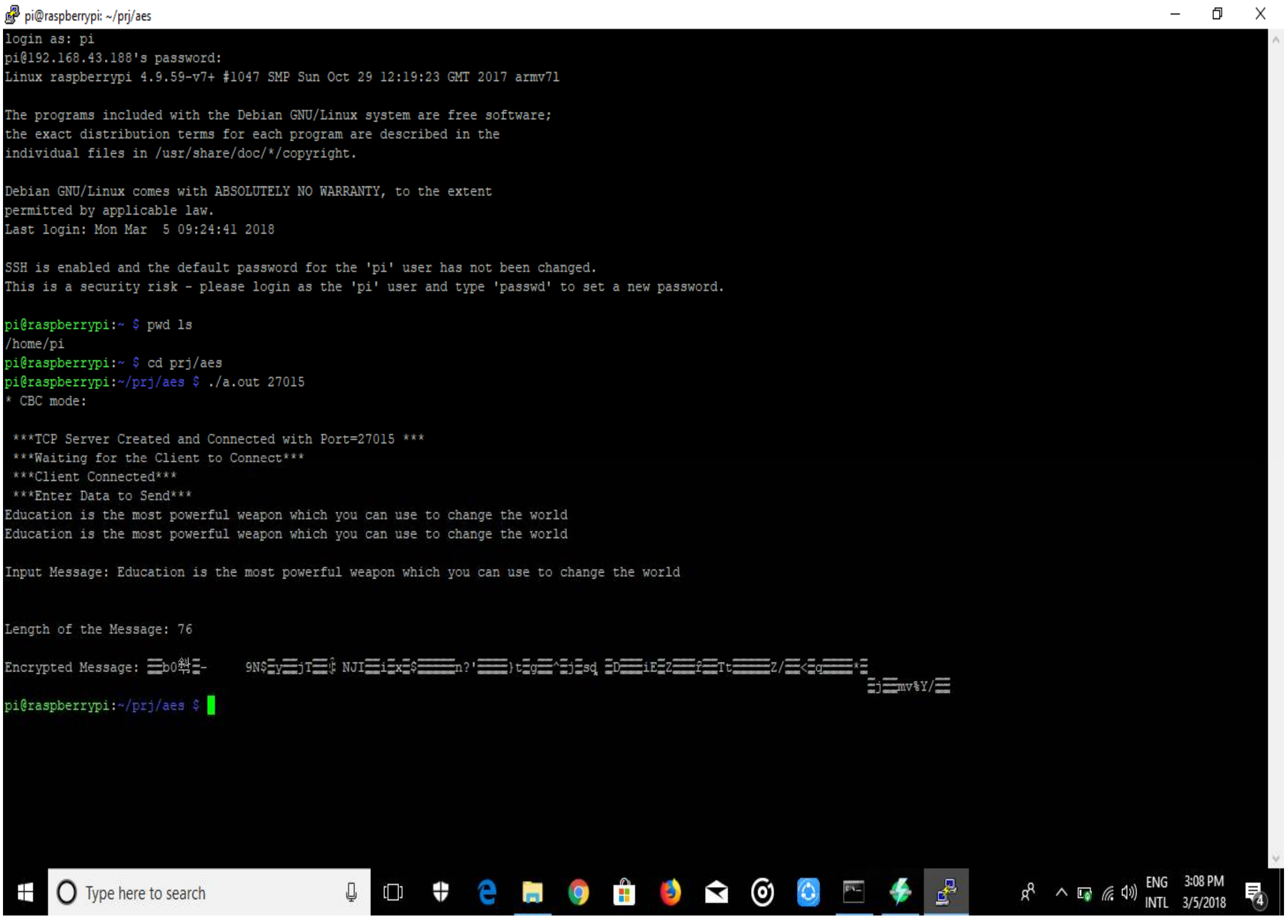
**Symmetric Key Cryptography**

In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key

**Asymmetric Key Cryptography**

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.

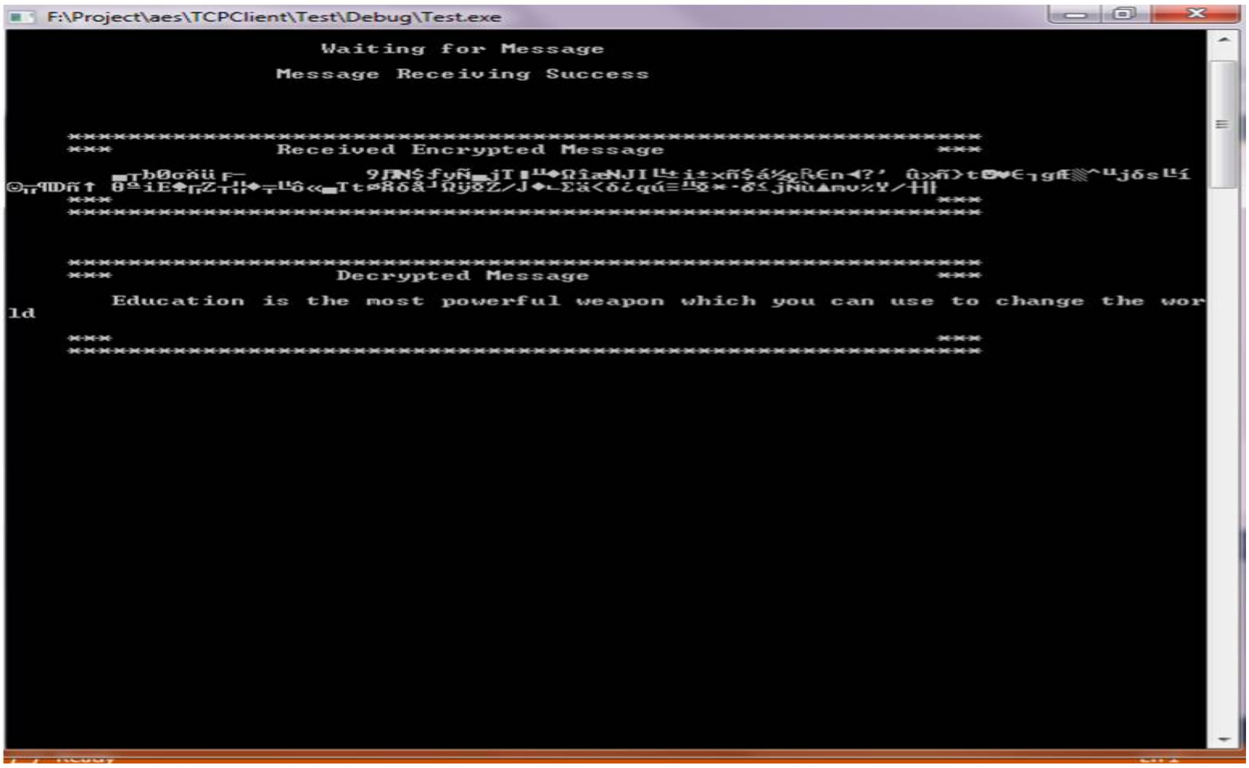
## V. RESULTS



```
login as: pi
pi@192.168.43.188's password:
Linux raspberrypi 4.9.59-v7+ #1047 SMP Sun Oct 29 12:19:23 GMT 2017 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar  5 09:24:41 2018

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $ pwd ls
/home/pi
pi@raspberrypi:~ $ cd prj/aes
pi@raspberrypi:~/prj/aes $ ./a.out 27015
* CBC mode:

 ***TCP Server Created and Connected with Port=27015 ***
 ***Waiting for the Client to Connect***
 ***Client Connected***
 ***Enter Data to Send***
Education is the most powerful weapon which you can use to change the world
Education is the most powerful weapon which you can use to change the world

Input Message: Education is the most powerful weapon which you can use to change the world


Length of the Message: 76

Encrypted Message: ☰b0斜☰-     9N$☰y☰jT☰‡ NJI☰i☰x☰$☰n?'☰}t☰g☰^☰j☰sq ☰D☰iE☰Z☰f☰Tt☰Z/☰<☰q☰*☰
                                                                                                            ☰j☰mv%Y/☰
pi@raspberrypi:~/prj/aes $
```

Fig. 9. Input data before Encryption

The above figure shows the input data before Encryption while giving the input messages according the secured communications.



```
                         Waiting for Message
                      Message Receiving Success


   ************************************************************
   ***               Received Encrypted Message             ***
        ▄╥b0σÄü╒─          9ƒN$ƒyÑ▄jT▐╙◆ΩîæNJI╚±i±xñ$á½çR€n◄?'  û»ñ>t☻♥€┐gÆ▒^╙jõs╙í
☺╥¶Dñ↑  θ≗iE♠╓Z╤╫◆╤╙ô«▄Tt≈Rôå┘Ωÿ≗Z/J◆└Σä<ô¿qú≡╧≗✶·ô≤jÑù▲mv%Y/╪╫
   ***                                                      ***
   ************************************************************


   ************************************************************
   ***                  Decrypted Message                   ***
     Education is the most powerful weapon which you can use to change the wor
ld
   ***                                                      ***
   ************************************************************
```

Fig. 10. Decrypted data after decryption

The above figure shows the decrypted data after decryption while the output data is shown according the secured communications.

## VI. Conclusion and Future Work

This paper shows successful implementation of text encryption as well as decryption . The AES Encryption algorithm is CBC mode is used here. The Advanced Encryption Standard is an iterative private key symmetric block cipher that can process data blocks of 128 bits through the use of cipher key with lengths of 128, 192 and 256 bits. An efficient 128 bit block and 128 bit key AES cryptosystem has been presented in the project using Raspberry Pi 3 Model B .The 128 bit data encryption and decryption is verified using Linux. The comparative performance benefit of a code is clearly shown here. The proposed methodology is applied for ensuring the personal privacy. Only authorized users that possess the key can decrypt the entire encrypted text. The proposed system can be extended to only authorized users can encrypt that possess the key can decrypt the entire encrypted image sequence, voice and video encryption as well as decryption. In this world of internet encryption of every multimedia data is primary need of all communication systems. In the same way this encryption technology will become the basic need for everyone.

## References

[1] V Patil, Prof.Dr.Uttam.L.Bombale ,P Dixit, “Implementation of AES algorithm on ARM processor for wireless network, ” in International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 8, August 2013,pp.3204-3209.

[2] X. Li, J. Chen, D. Qin, W. Wan Research and Realization based on hybrid encryption algorithm of improved AES and ECC, ”IEEE International Conference on Audio Language and Image Processing (ICALIP2010) (Nov 2010), pp. 396-400

[3] R. Pahal, V. kumar Efficient Implementation of AES, “International Journal of Advanced Research in Computer Science and Software Engineering”, 3(7) (July 2013), pp. 290-295

[4] Ajay Kushwaha, Hari Ram Sharma, Asha Ambhaikar, "A Novel Selective Encryption Method for Securing Text Over Mobile Ad Hoc Network" Procedia Computer Science, Volume 79, 2016, pp. 16-23

[5] V. Patil, Prof.Dr.Uttam.L. Bombale, P. Dixit Implementation of AES algorithm on ARM processor for wireless network, "International Journal of Advanced Research in Computer and Communication Engineering", 2 (8)(August 2013), pp. 3204-3209

[6] http://docs-europe.electrocomponents.com/webdocs/14ba/0900766b814ba5fd.pdf

[7] Sarita Kumar, IJECS Volume 6 Issue 4 April, 2017 Page No. 20915-20919

[8] file:///C:/Users/sastry/Downloads/3630-Article%20Text-6635-1-10-20180104%20(1).pdf

[9] http://www.ijettcs.org/Volume3Issue3/IJETTCS-2014-06-11-081.pdf

[10] http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

[11] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[12] http://www.engpaper.com/cryptography-2017.html

[13] https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryption