Implementation Scenerio of AES: Advanced Encryption Standered and Its Role

Girish Kumar[1]
Assistant, Professor

LPU, Phagwara
girish.21706@lpu.co.in

Dr. Ajay Shriram Kushwaha[2]
Associate, Professor

LPU,Phagwara
ajay.21908@lpu.co.in

Abstract— Today is the era of technology and information. Most important part of digital environment is encrypting the data so that secure information will received by the receiver. For this different techniques are implemented by computer scientists.

Moreover extensive research has being finished to explore the different technologies based on such secure mechanism environmental process. So many techniques are there but no one is reliable as more and more intruders are there to crack the system. This paper proposes a different approach to achieve encryption, AES:- Advance Encryption Standard using programming skills like Java to enforce cryptography.

Keywords—
Encryption, AES, intruders , Java

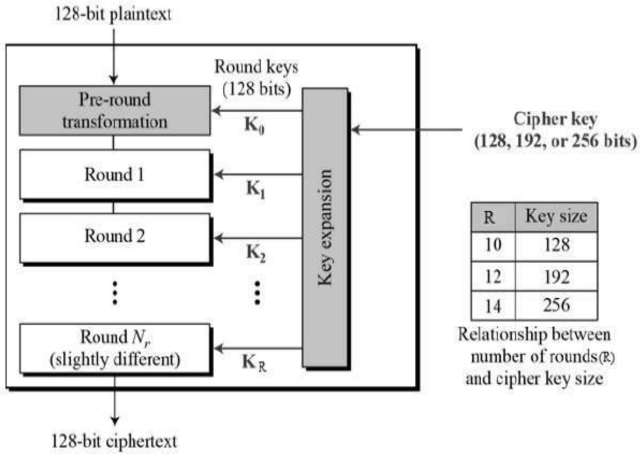
INTRODUCTION

AES or Advanced Encryption Standards ,is known since from last decade for secure encryption and decryption technique[1].Generally we have block cipher technique for secure encryption which is a base for AES method.

AES is also known as iterative in nature which make it more secure cipher technique. Like permutation and combination, we have n order outcome, just like it AES works[2]. i.e. it gives n outputs based on permutation and combination. AES contains an interconnected chain of work to do, some of which contain hidden participation by outer contribution yielding and others involves fresh arrangement of bits around it.

AES works with Bytes rather than bits, that is the main reason of success of AES-methodology. AES treats the one hundred and eight bits of a plaintext hinder as sixteen bytes. These sixteen bytes are orchestrated in four segments and four columns for preparing as a framework opposite to the technique available in DES, the incidence of processes in AES is changing parameter and depends upon the capacity of the key. AES performs with optimized way on ten scaled for 64*2-piece keys, twelve scaled for 92+100-piece keys and fourteen scaled for 128*2 -piece keys. Every one of these scaled utilizes an alternate 128-piece round key, which is determined from the first AES key.

Structure for AES is as:



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Fig:1 AES-Structure

Copyright © 2019Authors

ENCRYPTION TECHNIQUE

Following is diagrammatic representation of the general method of working of AES with diagrammatically which is quite understandable for the new user[2]

The first step process is shown below –

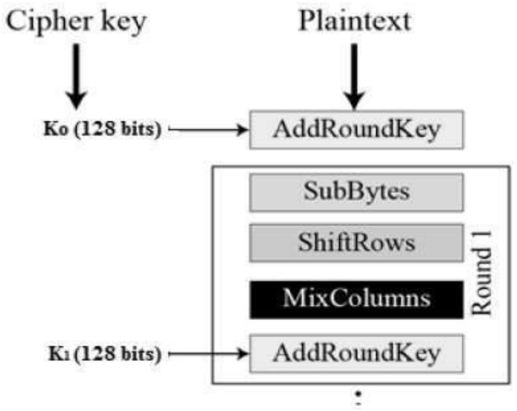


Fig:1 AES-Process

1) **SubByte (Byte substitution)**

The sixteen information bytes are given by checking into a fixed which is known as S-Table or S-Box and is given in the structure. The resultant is in a network of 8/2 lines and 8/2 sections.

2) **Shift-Rows:**

Every one of the 8/2 vertical value of matrix of the broad result is shifted to one side. Any sections that which is uncontrolled in manner is re-assembled on the exact supporting of line. Move is done as follow −

Un-shifted First Row

2nd row is shifted by single (byte) towards anti-right side

3rd row is shifted to 8/4 towards the anti-right.

And next task is, 4th horizontal value of matrix is shifted towards 21/7 positions to the anti-right.

Final result is a fresh lines consisting of the similar 8*2 bytes but moved with reference to each other

3) **Mix-Columns:**

All vertical values of matrix of 8/2 bytes is now formulated with the help of a special mathematical module. This procedure picks as input the 8/2 bytes of 8/8 column and outputs 8/2 fresh bytes, which alters the previous i.e. Original column. This will make a new matrix with 16 bytes.

4) **Add-Round-key:**

The 8*2*4 nibbles of the resultant are treated as 128*4 nibbles and are xored to the 128/8 bytes of the non truncated key. Cypher text will be considered if it is the last on, else, the remaining 128 bits are considered as 16 bytes and we begin another same task.

Anti-Encryption Mechanism

It is one of the best and easy ways to understand the fact that decryption process in the case of AES – methodology is the reverse of the process of encryption[3] process.

- Generating new non truncated key
- Mixing the vertical values
- Shifting horizontal values
- Byte assignments

Because every interleaved process in each round is exactly opposite in sense, as for a Feistel Cipher, the overall process of anti an non anti encryption method needs to be implemented on other way whether they are more and more close to each other

TECHONOLOGY USED:

Object Oriented approach -JAVA.

Because java is a robust language and some what is known for platform independent language so it is the most adequate language to use. Because of the extended usability of java in various applications we choose java. In the current era java holds a strong impact on application development. That so why java is so popular and easy to implement in the entire field. Due to socket programming availability in java we can use java in networking and with the implementation of AES algo in java, all the nut holds in communication seems to be perfect and running with smooth direction

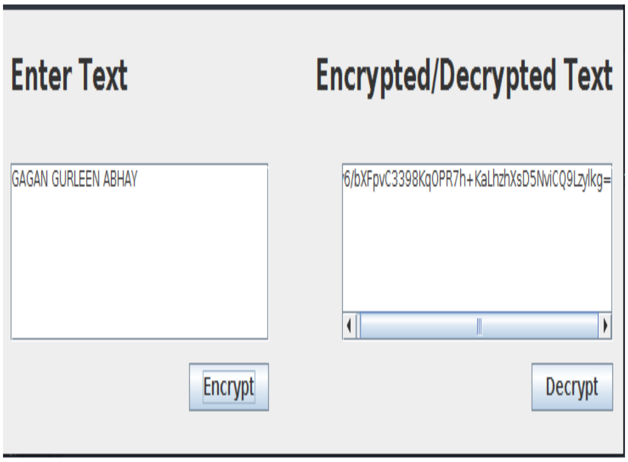
OBJECTIVES

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Our objective is to produce a highly secure cipher text with minimum use of efforts by implementing open source language. As there are so many protocols are available to tackle such type of strengthened encryption and decryption techniques but every code has its own advantages and disadvantages. AES is one of the best method available techniques so far and it is very easy to implement. Also AES is one of the best technique which pools with WiFi and other communication channels very easily[4].

SNAPSHOTS



GAGAN GURLEEN ABHAY

6/bXFpvC3398KqOPR7h+KaLhzhXsD5NviCQ9Lzylkg=

Fig: 3 Result after implementation

CONCLUSION

So it is concluded that after the implementation of AES – Algorithm, we can send the plain text via communication channel in such a secure way that our information tunnelling becomes quite difficult for the intruders. As java is open source so everyone can approach towards this technology.

REFERENCES

[1] John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―, 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[2] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips197.pdf.

[3] Verma," Peformance analysis of data encryption algorithms" International Conference on Electrical and Computer Technologies (ICECT), 3rd IEEE, Vol. 5, No.7, pp. 399 – 403, 2011

[4]Nagendra and Chandra Sekhar, "Performance Improvement of Advanced Encryption Algorithm using Parallel Computation",(IJSEIA), Vol.8, No.2, pp.287-296, ISSN: 1738-9984, 2014.

Copyright © 2019Authors