

Basics of AES Along with Newly Derived Encryption Logics

Panara Bhumita¹ Arpan Patel²

^{1,2}Department of Computer Engineering

^{1,2}Government Engineering College, Gandhinagar India

Abstract— As security of data is a crucial point nowadays. There are various causes that challenges the security of a data/network. Here in this paper we had tried to develop certain unique techniques of encryption. This paper shows brief glimpse on what encryption is and their standard algorithm also discusses how the newly derived technique can be useful.

Key words: Encryption, AES algorithm, need for encryption, derived logic.

I. WHAT IS ENCRYPTION?

Encryption is basically a conversion of electronic data into another form known as ciphertext. Ciphertext are kind of data that unauthorized parties can't understood [1].Encryption word means hidden or secret and is basically originated from Greekword 'kryptos'.

II. NEED FOR ENCRYPTION

Having a look to the older system of sending message ,it was observed that messages often used to get changed by intruder till it reach to the receiver, such cases may happen because of lack of security in those days. While comparing the procedure of sending message nowadays is also not safe even if seems it is, the reason is everything is sent through network which a hacker can hack to fetch the information sent through that network.

To resolve security problem, the term encryption comes into picture. It ensures that only the authorized parties can view the data. During transmission process it also ensures the confidentiality of the digital data stored in computer system when shared with other in the network. Developing the approach of encryption decreases the burden on the security of network, in the sense of even if data is hacked by someone then he/she won't get original information unless he/she has a solution to decrypt the ciphertext.

When plain-text is converted into ciphertext, the process is called encryption. Whereas when ciphertext is converted back to plain-text, the process is called Decryption.

The key used to encrypt the program is called encrypt key and the key used to decrypt the program is called decrypt key.

Encryption is a procedure that uses various algorithms to encrypt data. Algorithms generate key known as encrypt/decrypt key w.r.t encryption/decryption algorithm used.

Algorithms are divided into various categories on the basis of its functionality to encrypt any data.

A. Common block encryption algorithms:

- 1) AES(Rijndael)
- 2) Serpent
- 3) Cast
- 4) Triple DES
- 5) Blowfish
- 6) DES(Data Encryption Standard)
- 7) Twofish
- 8) Camellia
- 9) Idea

B. Common Stream Encryption Algorithms:

- 1) RC4

C. Common Cryptographic Hash Functions:

- 1) MD5
- 2) SHA-1
- 3) SHA-2
- 4) SHA-3(Keccak)
- 5) HAVAL
- 6) RIPEMD
- 7) Tiger
- 8) WHIRLPOOL

Note: To encrypt the documents ‘Block ciphers’ work on blocks of data and ‘Stream ciphers’ are used to encrypt streams of data such as chat programs.[1]

In this paper we are focusing on two algorithm namely:

- AES

III. AES (RIJNDAEL):

A. History:

AES stands for Advanced Encryption Standard. Due to limitations of DES algorithms such as block sizes and small key. NIST (National Institute of Standards and Technology) decided to select new block cipher and search for new process. Among 15 proposals ‘Rijndael’ was selected and was chosen as AES from 2001 onwards.

Rijndael was chosen for its efficiency, implementability, security and flexible performance as compared to DES. AES has a fairly simple algebraic description. [3] As of July 2009, no practical attacks have been successful on AES. Except side channel attacks that occur due to weakness found in key management and implementation. [4]

1) Platform Requirements:

AES works on 8-bit smart card to high performance computers. This a quite wide range of portability which makes ‘Rijndael’ an advanced version of DES.

2) Limitations on string input:

AES works for different ranges of string such as 128 bits, 192 bits and 256 bits. Different rounds are traversed for specific range of string.

3) Time required to encrypt:

High Speed and low RAM requirements. AES encryption requires 18 clock cycles per byte on a Pentium pro, which is almost equal to a throughput of about 11MB/s for a 200 MHz processor. Also the throughput is about 60 MB/s on a 1.7 GHz Pentium M. [3]

IV. RIJNDAEL ALGORITHM

AES is based on substitution permutation network also it is an iterative rather than Feistel cipher.

All the operations are performed on bytes rather than bits. As a result it deals with 16 bytes in place of 128 bits plaintext block. Hence, 16 bytes forms a matrix of 4*4.

Whole process is run into number of rounds based on no of bits as below:

No of Bits	Rounds
1. 256	14
2. 192	12
3. 128	10

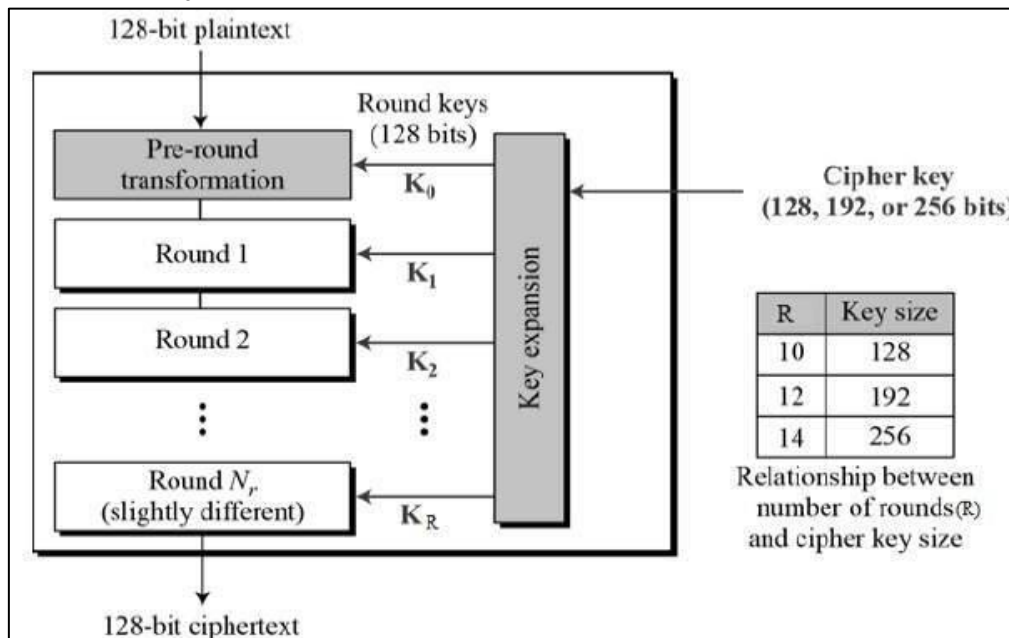


Fig. 1: Rounds of encryption

The whole process is divided in 4 rounds:

- 1) Byte Substitution
- 2) Shift Rows
- 3) Mix Columns
- 4) Add round key

A. Byte Substitution:

A matrix is formed of 4 rows and 4 columns.

B. Shift Rows:

Each 4 rows of matrix is shifted to left. Shifting is done in various ways as per row number for example first row is not shifted whereas 2nd row by 1 shift, 3 row by 2 shifts and 4th by 3 shifts. As a result new matrix is formed containing same 16 bytes.

C. Mix Columns:

In this, elements of each columns is transformed into some another number using mathematical functions and a new matrix with updated row element is formed.

This step must not be repeated in the last round.

D. Add Round Key:

The 16 bytes of the matrix are now taken as 128 bits and are XORed to the 128 bits of the round key. Output is the ciphertext, if this is the last round. Otherwise, the resulting 128 bits are interpreted as 16 bytes. [2]

E. Algorithm:

- 1) Step 1: Implement AES Algorithm as explained above.
- 2) Step 2: Encrypted String so obtained while processing Rijndael algorithm is given as an input to another logic.
- 3) Step 3: Convert each character of obtained string into its corresponding alphabet no.
- 4) Step 4: Add 3 (+3) to alphabet no. of each character.
- 5) Step 5: A series with new alphabet no. is formed.
- 6) Step 6: Fetch back the string from new series of alphabet no.
- 7) Step 7: Now assign each character of string with Fibonacci Series. (i.e. 0, 1, 1, 2, 3, 5...)
- 8) Step 8: After assigning Fibonacci no. to each character, rail fence is generated as below:
 0-----1-----3-----8-----21
 1-----2-----5-----13-----34
- 9) Step 9: Again assign each character of string with rail fence no.
- 10) Step 10: Note down the alphabet no so obtained from step 5.
- 11) Step 11: Add rail fence no obtained from step 9 to alphabet no. obtained from step 10. (Rail fence + Alphabet no)
- 12) Step 12: Each character is assigned to new no after processing step 11. (Check whether if total exceeds 26 then subtracts 26 to get actual no.)
- 13) Step 13: Consider output of step 12 as alpha no. now fetch the character from the corresponding alphabet no.
- 14) Step 14: String so obtained is encrypted string.

The Snapshot showing C implementation of algorithm is as below:

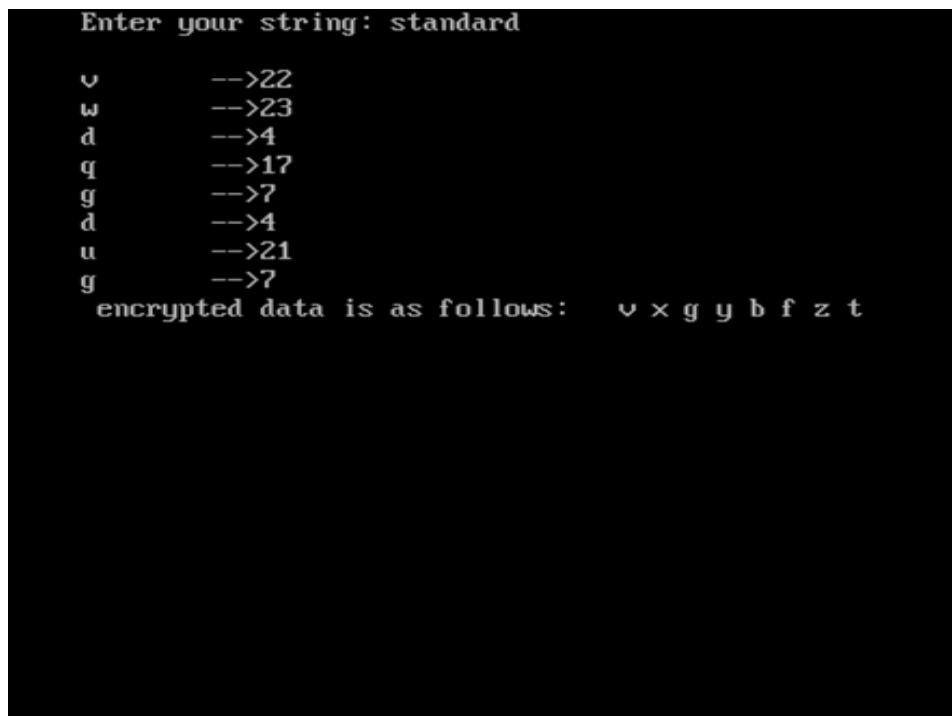


Fig. 2: Program execution

Given algorithm so formed is strong as it uses Rijndael algorithm in addition with other logics such as Fibonacci and rail fence.

The procedure to encrypt the string “Encrypt” is explained below:

Input String: Encrypt

Step 1: Original Alpha no +3

E - 5	+3 => 8		=> H
N - 14	=>17		=> Q
C - 3	=>6		=> F
R - 18	=>21		=> U
Y - 25	=>28-26=2		=> B
P - 16	=>19		=> S
T - 20	=>23		=> W

New String formed: H Q F U B S W

Step 2: Fibonacci Series

0	1	1	2	3	5	8
H	Q	F	U	B	S	W

Step 3: Rail Fence

0	1	3	8	21	1	2
H	Q	F	U	B	S	W

Step 4: Alphabet No.

H	Q	F	U	B	S	W
8	17	6	21	2	19	23

Step 5: Rail Fence + Alphabet number

8	18	9	29	23	20	25
H	R	I	C	W	T	Y

F. Benefits of using this algorithm:

Algorithm provides all the features of AES, its performance get improve when other logics are added and makes the algorithm difficult to trace out.

When such encryption algorithm is used in sending messages through network the intruder would try to decrypt it using common or standard decryption methods available.

G. Using the above algorithm serves the goodness of following features:

- It doesn't increase the execution time while implementing on c language. It is quite faster.
- It encodes and varies the encrypted output string from Advanced Encryption Standard algorithm 'Rijndael' in such a way that it's quite hard for the hacker to crack it.
- The combination of various techniques used here is unique.
- The C/Java implementation of above (derived) algorithm is possible.
- The algorithm works from all type of string inputs.
- The logic is simplified one even though hard to crack the sequence in which it is used.
- Such logic along with AES can be used in making application for mobile that stores data in encrypted form. One with knowledge of making android app can make a simple interactive app that just simply provide encryption to the data entered.

V. CONCLUSION

The algorithm derived in the paper can be used in combination with other algorithms too. Encryption is a solution to many security threats. Rijndael as an AES has great security strength along with many compatible features.

ACKNOWLEDEMENT

We would like to articulate our deep gratitude to my thesis guide Asst. Prof. S. M. Bhandari who has guided us in our paperwork. I really appreciate the keen interest for encouraging all time for our paperwork to Associate Prof. Kajal S. Patel, Professor and Head of Computer Engineering Department of Government Engineering College, Rajkot, Gujarat.

REFERENCES

- [1] <https://security.stackexchange.com/questions/54835/current-encryption-algorithms>
- [2] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
- [3] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- [4] <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>