Middle-East Journal of Scientific Research 24 (4): 1325-1329, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.04.23301

Hybrid AES Algorithm Using 16 Fiestel Based Network with Distinct Keys

[1]P.G. Gopika, [2]N. Hariharan and [3]S. Perumal Sankar

[1]Adi Shankara Institute of Engineering and Technology, Kalady, Kerala, India
[2]Dean of PG Studies, Adi Shankara Institute of Engineering and Technology, kalady, Kerala, India
[3]Professor, TOC H Institute of Tehnology

Abstract: In this work, a method to improve the security of existing cryptographic system is proposed. Here hybrid AES algorithm which make use of AES with Feistel network and distinct keys are employed. This hybrid algorithm propose16 rounds for AES-128 thereby security is enhanced as compared to existing system. This algorithm use AES key generation method for standard AES 128 and a predefined key for feistel network. Confusion provided by this system is much better than the technology prevalent in the existing systems.

Key words: AES · DES · Hybrid algorithm

INTRODUCTION

The rapid growth of secure transmission is a critical point nowadays. We have to exchange data securely at very high data rates [1]. Cryptography is an important tool in modern electronic security technologies to protect valuable information resources on intranets, extranets and the Internet. It has been used historically as a means of providing secure communication between individuals, government agencies and military forces.

Cryptography is mostly concerned with keeping messages secret. Cryptography is the art of transforming a readable text (plain text) into an unreadable one (cipher text) which ensures data privacy. The word "crypto" means "hidden" and "graphy" means "to write". It is concerned with information security, data encryption, data authentication and access control. Nobody then should be able to obtain the plaintext from the cipher text without knowing the key. The method of transforming plaintext to cipher text is called encryption and the method itself is called the encryption algorithm (or cipher system) [2].

They can be categorized into Symmetric (secrete) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used. private and public keys . Public key is used for encryption and private key is used for decryption (e.g. RSA). Public key encryption is based on mathematical functions, computationally intensive [3] AES is the most popular symmetric key block cipher used today. It uses a block size of 128 bits with a variable key length of 128 bits, 192 bits or 256 bits. While DES and many other ciphers used a Feistel network, AES uses a substitution permutation network. This substitution-permutation network allows AES to perform fast in both software and hardware applications. AES is simple to implement and uses very little system memory. But now a day's AES face more attack especially algebraic attack. One of the best solution to overcome this attack is use a hybrid AES algorithm with feistel based network. It provide more security than the standard AES.

Hybrid Aes Using Feistel Based Network with Distinct Key: Figure 1 depicits the structure 9of the proposed system where the inputs to the algorithm are a plain text of 256 bits and a predefined key. The basic idea of the hybrid AES using Feistel based network with ditinct key model is to integrate AES into each iteration of the Feistal network of DES. Mathematically, each round of the model can be expressed as:

$$Ln = Rn\text{-}1 \quad (1)$$

$$Rn = AES\ (Ln\text{-}1 \text{ xor } Rn\text{-}1 \text{ xor } Kn) \quad (2)$$

The above set of equation is repeated over each of the 10 rounds [4].

Corresponding Author: P.G. Gopika, Adi Shankara Institute of Engineering and Technology, Kalady, Kerala, India.

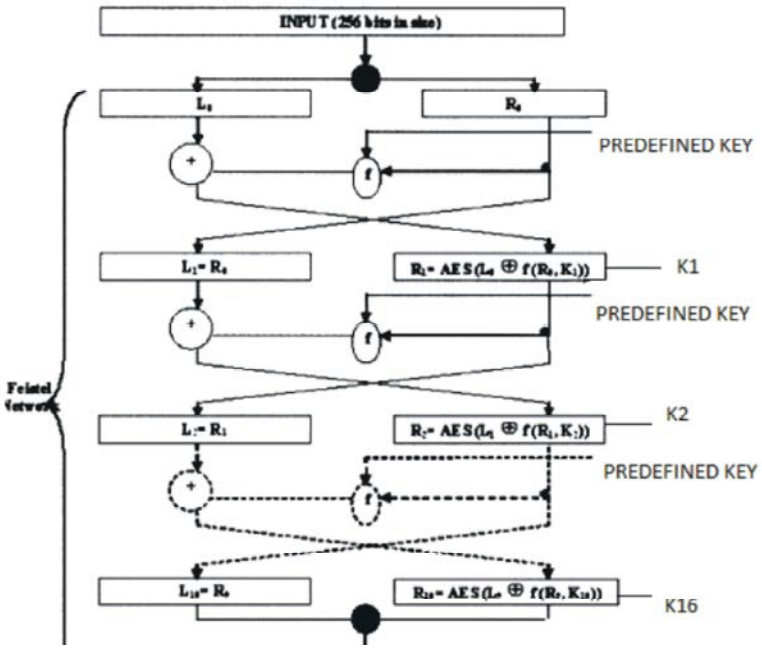

Fig. 1: Proposed network

The plain text 256 bits is initially divided into two halves, left and right. For each round three variables are XORed according to the equation (2). The resulting variable uses the input of the AES. The AES function includes sub byte, shift row, mix column, add round key. Left half portion is simply the right half of the previous round. AES processes are described below.

Sub Byte [5, 6]: Each input byte of the State matrix is independently replaced by another byte from a look-up table called S-Box shown in Fig. 2.1. The substitution byte for each input byte is found by using the S-Box lookup table. The size of the lookup table is 16×16. To find the substitute byte for a given input byte, we divide the input byte into two 4-bit patterns, each yielding an integer value between 0 and 15 which can represent these by hex values 0 through F. One of the hex values is used as a row index and the other as a column index for reaching into the 16×16 lookup table [5]. The entries in the lookup table are constructed by a combination of GF(28) arithmetic and bit scrambling. The goal of the substitution step is to reduce the correlation between the input bits and the output bits. The bit scrambling part of the substitution step ensures that the substitution cannot be described in the form of evaluating a simple mathematical function [6].

Shift Row [5]: In the Shift Row transformation, the bytes in the last three rows of the State are cyclically shifted over l, 2 and 3bytes respectively as shown in Fig. 2.2. In Shift Rows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left [5].

Mix Columns [5]: The Mix Columns transformation operates on the State column by column, treating each column as a four-term polynomial.

It is based on Galois field (GF) multiplication. Each byte of a column is replaced ith another value that is a function of all four bytes in the given column [7]. As a result of the Mix Column transformation, the four bytes in a column are replaced by the following four bytes [8, 9];

S'0, c=({02}*So, c) ^({03}*S1, c) ^ S2, c ^S3, c

S'1, c= S0, c ^({02}*S1, c) ^({03}*S2, c) ^S3, c

S'2, c=S0, c ^S1, c^ ({02}*S2, c) ^ ({03}, S3, c)

S'3, c=({03}*S0, c) ^S1, c ^ S2, c ^({02}*S3, c)

Add Round Key [6]: The Add Round Key phase performs an operation on the State with one of the sub keys. The operation is a simple XOR between each byte of the State and each byte of the sub-key.

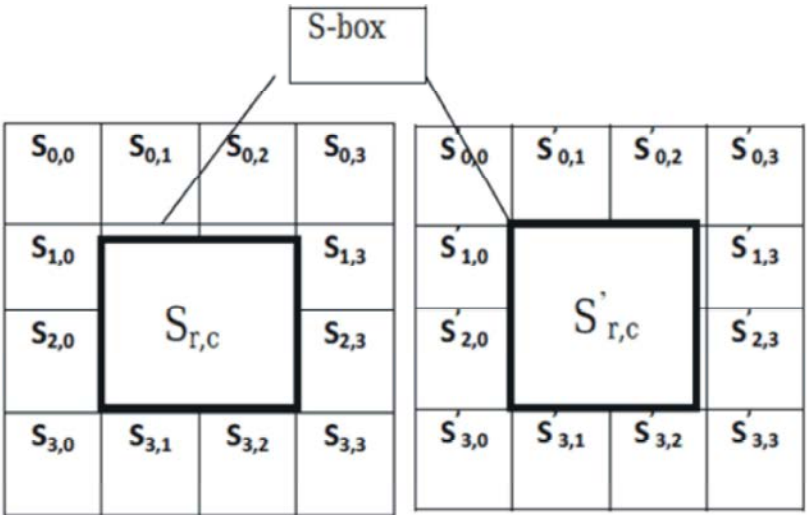

Fig. 2.1: Look up table for Substitution box

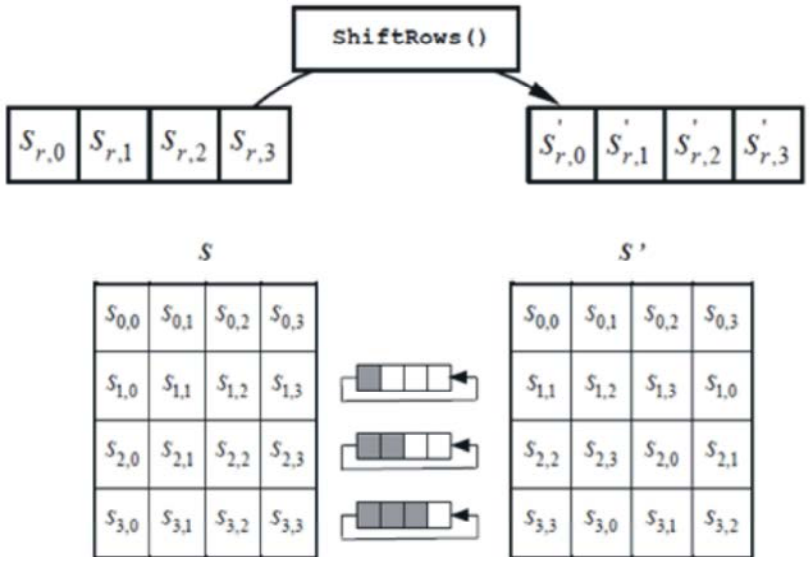

Fig. 2.2: Shift Row

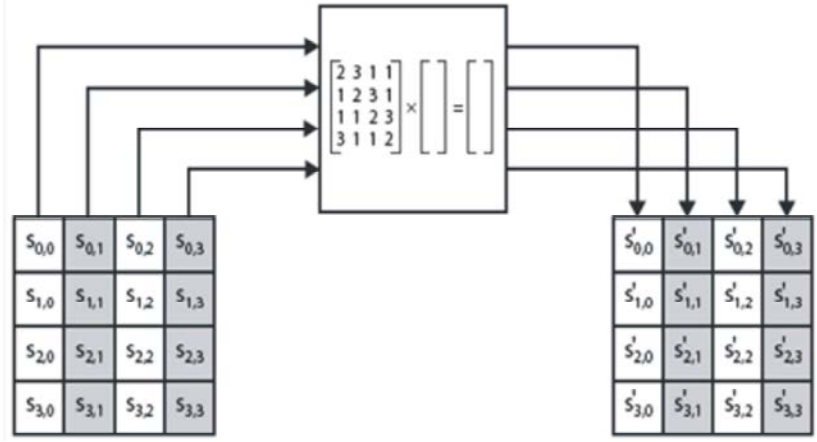

Fig. 2.3: Mix Columns

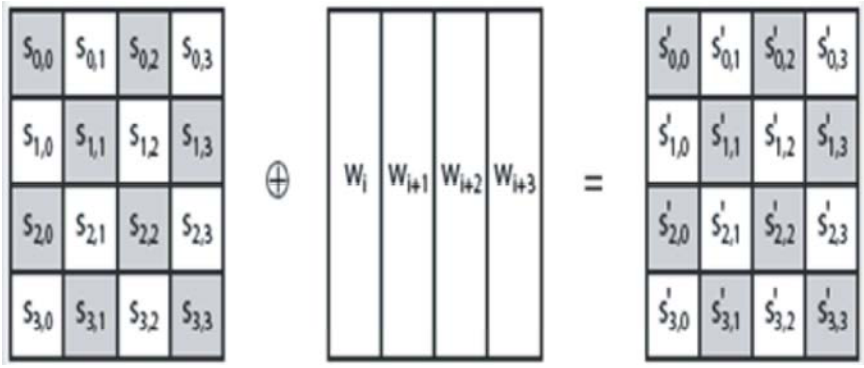

Fig. 2.4: Add Round Key

Hybrid algorithm use 16 layers for AES 128 and different sets of keys for Feistel and AES of hybrid algorithm. The proposed algorithm is more secured than existing hybrid AES- DES algorithm. Number of rounds depend on the level of security we need. By employing more number of rounds, we can enhance the data transmission security and vice-versa. The different sets of key will further enhance the security level of the system. For AES, process key is generated from standard AES but for the Feistel network, a predetermined key is used. Result show that confusion produced by this method is much greater than the existing method and produce a good avalanche effect.

RESULTS

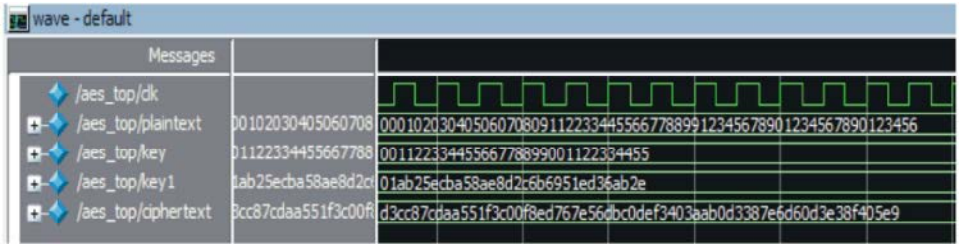

Fig. 3.1: Encryption

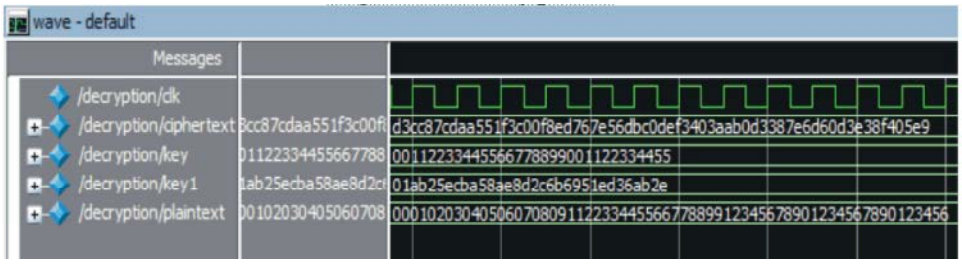

Fig. 3.2: Decryption

Encryption and decryption is done using Model Sim. Length of plain text and cipher text are 256 bits. Length of key and key1 are 128 bits. Data used for functional verification are:

Plain Text:

000102030405060708091122334455667788991234567890123456789012345678901234567890123456

Key: 00112233445566778899001122334455

Key1: 01ab25ecba58ae8d2c6b6951ed36ab2e

Fig. 3.1 shows that confusion property is much higher as compared to existing technology. Fig. 3.2 shows that after decryption, the plain text can be recovered by using the same key and key1.

The result show that 16 rounds performing 4 distinct transformation functions increases the confusion property of the algorithm. Security of the system depends on Feistel key strength. System security can be improved further by using 16 different keys for Feistel network.

CONCLUSION

In hybrid AES using Feistel network , 16 rounds performing 4 distinct transformation functions and single key is used for both feistel network and aes. In this work, we made certain modification for improving the security. In this method, number of rounds performing the transformations are increased to 16 and two different keys are used for both AES and Feistel . A predefined key is used for Feistel network. Through this modification, we have shown that security of the cryptographic system is improved. Confusion provided by this system is much better than the technology prevalent in the existing systems.

REFERENCES

1. Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, and Jean-Didier Legat, 2003. "Efficient Uses of FPGAs for Implementations of DES and Its Experimental Linear Cryptanalysis", IEEE Transactions on Computers, 52(4).
2. Sourabh Chandra, Siddhartha Bhattacharyya, 2014. "A Study and Analysis on Symmetric Cryptography" IEEE-International Conference on Science, Engineering and Management Research.
3. Dr. Prerna Mahajan and Abhishek Sachdeva, 2013. "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, 13(15) Version 1.0 Year 2013.
4. Vishnu, M.B., S.K. Tiong and S.P. Koh, 2008. "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", Communication, APCC 2008. 14th Asia-pacific Conference.
5. Rahul Gandh, D. and V. Kamalakannan, 2014. "FPGA Implementation of Enhanced Key Expansion Algorithm for Advanced Encryption Standard", International Conference on Contemporary Computing and Informatics, IEEE.
6. Hrushikesh S. Deshpande, Kailash J. Karande and Altaaf O. Mulani, 2014. "Efficient Implementation Of Aes Algorithm On Fpga", International Conference on Communication and Signal Processing, April 3-5, 2014, India.
7. Dr. Diaa Salama, Hatem Abdelkader amd Mohiy M. Hadhoud, 2009. "Performance Evaluation of Symmetric Encryption Algorithms", Article in International Journal of Network Security.
8. Anurhea Dutta, Prerna Bharti, Swati Agrawal and K.S. Surekha, 2012. "Hybrid AES-DES Block Cipher: Implementation using Xilinx ISE 9.1i", UACEE International Journal of Advancements in Electronics and Electrical Engineering, 1(2).
9. Behrouz a forouzan and Debdeep Mukhopadhyay, "Cryptography And Network Security", Second Edition, 2010.