ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 8, October 2012

A Novel Approach to Improve Avalanche Effect of AES Algorithm

Chandra Prakash Dewangan,Shashikant Agrawal

Abstract— **With the rapid progression of digital data exchange in electronic way, security of information is becoming more important in data storage and transmission. Therefore numerous ways of protecting information are being utilized by individuals, businesses, and governments. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. This security system uses some algorithms to scramble data into scribbled text which can be only being decoded or decrypted by party those possesses the associated key. In this paper a most widely used symmetric encryption techniques i.e. advanced encryption standard (AES) have been implemented using MATLAB software. The primary goal of this paper is to improve level of security. The implemented encryption technique is analyzed by using a parameter called Avalanche effect. Plaintext and encryption key are mapped in binary code before encryption process. Avalanche Effect is calculated by changing one bit in plaintext keeping the key constant and by changing one bit in encryption key keeping the key constant, Experimental results shows that the proposed algorithm exhibit significant high Avalanche Effect which improves the level of the security.**

Keywords*— *Advanced Encryption Standard (AES), Avalanche Effect, Ciphertext, Secret key.

I. Introduction

Transmission of sensitive digital data over the communication channel has emphasized the need for fast and secure digital communication network to achieve the requirement for integrity, secrecy and non reproduction of transmitted information. The main goal of cryptography is to keep the data secure from unauthorized access. Cryptography provides a scheme for securing and authenticating the transmission of information across insecure communication channels. It enables us to store susceptible information or transmit it over insecure communication networks so that unauthorized persons cannot read it. [1] A Cryptographic method of scrambles the content of digital data like text, image, audio and video to make it unreadable or unintelligible for others during transmission. [2] A system that performs encryption decryption is called cryptosystem. The complexity of encryption process depends on algorithm used for encryption, software used and the key used in algorithm to encrypt or decrypt the data [3]. There are chiefly two types of cryptographic algorithms: symmetric and asymmetric algorithms. Symmetric systems e.g. Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) uses same key for the sender and receiver both to encrypt the information and decrypt the cipher text. Asymmetric systems e.g. Rivest-Shamir-Adelman (RSA) & Elliptic Curve Cryptosystem (ECC) uses different keys for encryption and decryption. Symmetric cryptosystems is more appropriate to encrypt large amount of data with high speed.

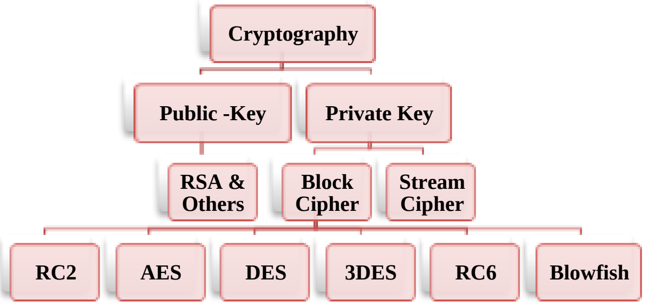

Fig 1 Overview of the field of cryptography

After far-reaching survey of various research papers it is observed that an encryption algorithm should produce significant change in the encrypted message when a small change is made in original message. In research papers [8] and [9] authors analyzed various cryptographic algorithms using a parameter called Avalanche Effect. In this paper we proposed an enhancement in AES algorithm using binary codes. This proposed algorithm is expected to provide significant high Avalanche Effect.

II. Cryptography

Depending upon the number of keys used, cryptographic algorithms can be classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). In Symmetric keys encryption or secret key encryption identical key is used by sender and receiver. Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) are the example of Symmetric key encryption algorithms. In Asymmetric keys encryption two different keys (public and private keys) are used for encryption and decryption. Public key is used for encryption and private key is used for decryption.Rivest-Shamir-

Manuscript received Sep 15, 2012.

Chandra Prakash Dewangan, *M.E. scholar, Department of Electronics and Telecommunication Chhatrapati Shivaji Institute of Technology, Durg,India,+91-9179198168*
Shashikant Agrawal, *Department of Electronics and Telecommunication Chhatrapati Shivaji Institute of Technology, Durg,India,*

Adelman (RSA) and Elliptic Curve Cryptosystem (ECC) is the example of asymmetric key algorithms. [4]

A symmetric cryptosystem has five ingredients:

A. Plain text

This is the original data or message to be transmitted that fed into the algorithm as input.

B. Encryption Algorithm

The algorithm performs various transformations and substitutions on the plaintext.

C. Secret key

This is another input to the algorithm and the value of secret key is independent of the plaintext. Depending on the specific key the algorithm will produce a different output.

D. Cipher Text

This is the scrambled or encrypted message produced as output. This output depends on the plaintext and the secret key.

E. Decryption Algorithm

This is essentially the encryption algorithm operate in reverse. It takes the ciphertext and the secret key as input and produces the original plaintext as output. [5]

III. AES Algorithm

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is supple in supporting any combination of data and encryption key size of 128, 192 or 256 bits. However, AES only allows a 128 bit data length that can be divided into four basic operational blocks. These blocks operate as array of bytes and organized as a matrix of the order of 4x4 that is called the state. For encryption process, the data is passed through Nr rounds (Nr = 10, 12, 14) [6, 12, 13].

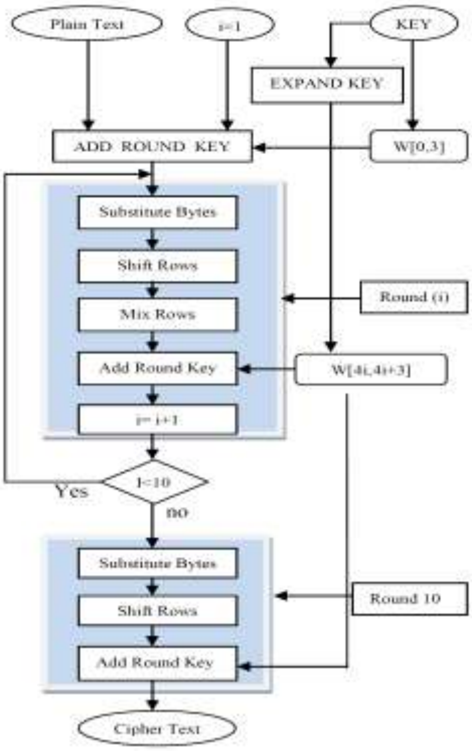

Fig. 2 AES (Advanced Encryption Standard) process

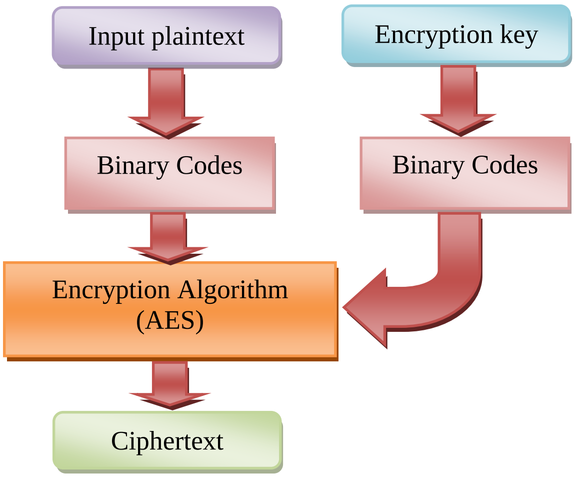

Fig 3 AES process when input plaintext and input key are mapped in various binary code

To provide security AES uses types of transformation. Substitution, permutation, mixing and key adding each round of AES except the last uses the four transformations .Figure 2 shows flowchart for AES process.

Each round of AES is governed by the following transformations.

A. Bytesub transformation

It is a non linear byte Substitution, which is performed using a substitution table (s-box). Multiplicative inverse and affine transformation are used to construct S-Box.

B. Shiftrows transformation

It is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift ranges from one to three bytes.

C. Mixcolumns transformation

It is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

D. Addroundkey transformation

It is a simple XOR between the working state and the round key. This transformation is its own inverse.

The encryption procedure consists of above steps. Initially an addroundkey operation is performed. After that a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on length of the key. The decryption process has exactly the same sequence of transformations as performed in the encryption process.

IV. Methodology

In the proposed algorithm we have changed the form of plaintext and encryption key given to the AES algorithm. Instead of giving plaintext and Encryption key directly, we have mapped input plaintext and input encryption key in various binary codes before being applied to the input of the AES algorithm. Some of these binary codes are weighted and some are unweighted. [7] Figure 3 shows the block diagram of algorithm that we have used for our experiments.

If there are n quantities in a group, a code of binary digits or bits may represent all quantities unequally.

$$N \leq 2^b$$

A. *Natural BCD Code (8421 code)*

Natural BCD code or 8421 code is used whenever decimal information is transferred in or out of a digital system. In this code straight assignment of binary equivalent is used with weights.

B. *2421 Code*

These are weighted ,reflected and self-complementing codes, In 2421 codes if a number has more than one representation then o choose the code that uses the lower binary weights (for number 0-4 only)

C. *5421 Code*

These are weighted code with weight 5-4-2-1. In 5421 codes if a number has more than one representation then choose the code that uses the lower binary weights.

D. *7421 Code*

These are weighted code with weight 7-4-2-1. For decimal number 7 choose code with least number of 1's.

E. *5311/5211 Code*

These are weighted code with weight 5-3-3-1. In 5331 codes if a number has more than one representation then choose the code with least number of 1's and use first the 1 from extreme right that uses the lower binary weights.

F. *Gray code*

It is also known as "reflected and unit distance code" which is a reflected mirror image. Unit distance exhibit only a single bit change from one code to the next. It is also an unweighted and not an arithmetic code.

G. *3321/4221 Code*

These are weighted code with weight 3-3-2-1/4-2-2-1.

V. Evaluation Parameters

Each of the encryption technique has its own strong and weak points. In order to apply an appropriate technique in a particular application we are required to know these strengths and weakness. Therefore the analysis of this technique is critically necessary. A enviable property of any encryption algorithm is that a small change in either the plaintext or the key must produce a significant change in the cipher text. However, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts. This property is known as Avalanche effect [8, 9].

$$\boxed{\text{Avalanche Effect} = \frac{\text{Number of flipped bits in ciphered text}}{\text{Number of bits in ciphered text}}}$$

The performance of proposed algorithm is evaluated using Avalanche Effect due to one bit variation in plaintext(before being mapped in various binary codes) keeping encryption key constant in a binary code and Avalanche Effect due to one bit variation in encryption key(before being mapped in various binary codes) keeping plaintext constant in a binary code. Figure 4 shows the evaluation of Avalanche Effect

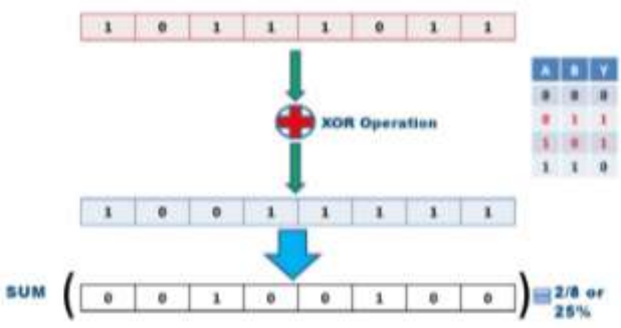

Fig.4 Calculation of Avalanche Effect

TABLE I. AVALANCHE EFFECT OF AES WITHOUT MAPPING IN BINARY CODES

1 bit variation in plaintext keeping the key constant	1 bit variation in key keeping the plaintext constant
73	77

VI. Experimental Result and Analysis

We have been implemented AES algorithm using MATLAB 7.0 Software. Input to the algorithm is a block of 128 bit plaintext (data) and a 128 bit encryption key. Analysis for Advanced Encryption Standard (AES) algorithm is shown in following tables. The original data to be encrypted and thy key used for encryption are mapped into various binary codes before encryption process.

After implementation, we have been calculated the Avalanche Effect for both the AES algorithm and the proposed algorithm (when plaintext and encryption key being mapped in various binary codes) for different combination of binary codes.

Table I shows Avalanche Effect due to 1 bit variation in plaintext keeping the key constant and Avalanche Effect due to 1 bit variation in key keeping the plaintext constant.

Table II shows the Avalanche Effect when input encryption key is kept fixed in different binary code and one bit of the plaintext is flipped before being mapped in binary codes. Avalanche Effect is calculated by counting the number of flipped bits in the cipher text due to one bit change in the original plaintext before being before being mapped in binary code while key remains constant in a binary code throughout the experiment.

It is clear from table II that avalanche effect is maximum (i.e. 81 bit out of 128 bits) when both key and data are mapped in 8421 binary code.

Table III shows the avalanche effect when data kept fixed in a binary code and key is varied in different codes. It is

TABLE II - KEY KEPT FIXED IN SAME CODE ANDDATA CODE VARY

Data ↓	Key in Format								
	2421	**3321**	**4221**	**5211**	**5311**	**5421**	**7421**	**GRAY**	**8421**
2421	61	63	56	66	65	62	69	54	60
3321	64	63	62	68	70	64	56	68	61
4221	58	61	66	71	59	61	62	63	61
5211	67	71	60	69	64	65	66	55	65
5311	64	57	68	66	68	58	62	68	62
5421	71	57	68	62	65	61	68	71	65
7421	67	69	58	72	62	57	75	56	71
GRAY	54	70	60	67	61	63	69	69	68
8421	64	65	67	72	61	70	69	62	**81**

TABLE III - PLAINTEXT KEPT FIXED IN SAME CODE AND KEY CODE VARY

Key ↓	Data in Format								
	2421	**3321**	**4221**	**5211**	**5311**	**5421**	**7421**	**GRAY**	**8421**
2421	63	62	61	59	54	71	69	66	60
3321	67	66	59	64	70	56	58	**77**	62
4221	58	66	62	61	62	68	62	68	58
5211	67	69	62	59	55	74	64	60	59
5311	58	63	67	58	71	69	64	74	59
5421	52	64	60	63	64	66	71	62	76
7421	61	67	69	64	66	75	63	64	64
GRAY	65	72	65	71	77	61	72	68	59
8421	62	57	70	61	62	66	57	64	66

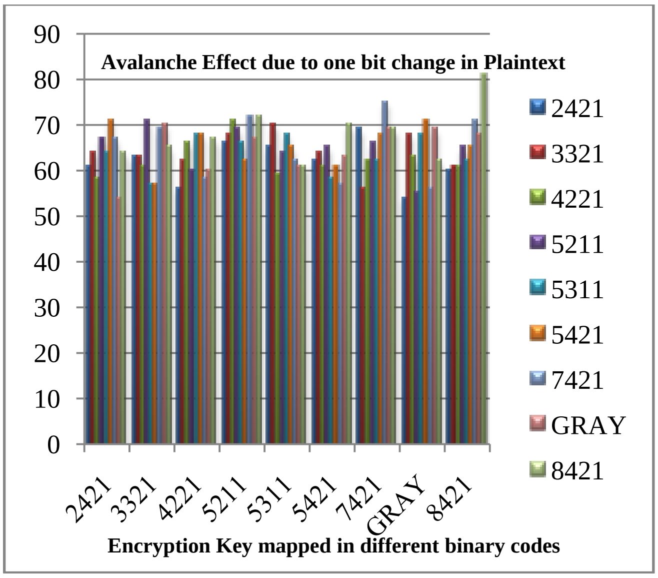

Fig 5 Analysis of Avalanche Effect Due to one bit change in plaintext

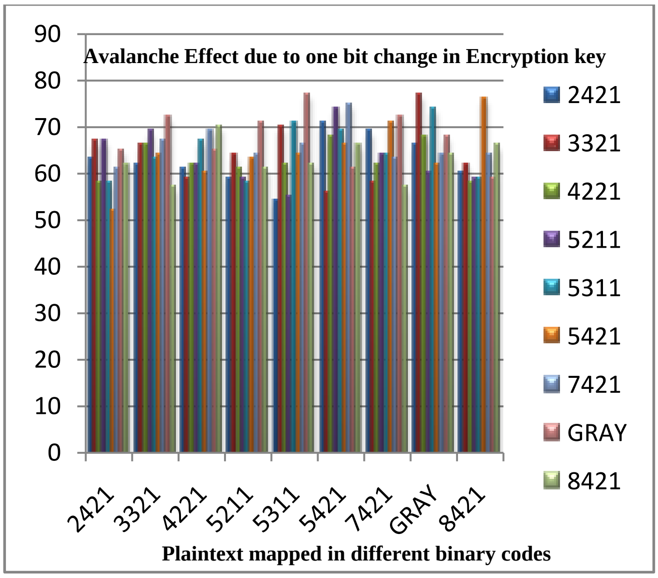

Fig 6 Analysis of Avalanche Effect Due to one bit change in Encryption Key

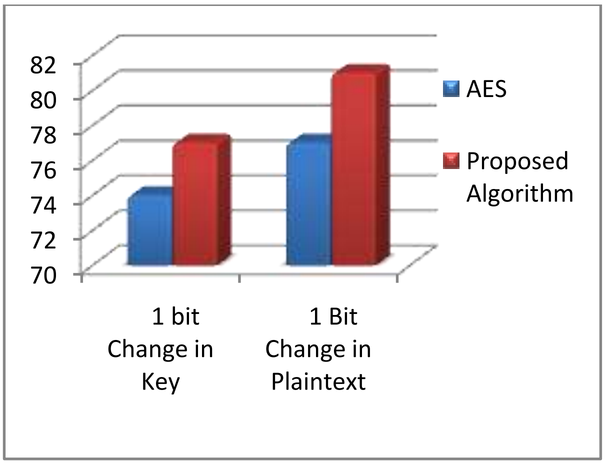

Fig 7 Comparison between avalanche effect of AES and Proposed Algorithm

clear from table III that avalanche effect is maximum (i.e. 77 bit out of 128 bits) when data remain fixed in gray code and 1 bit is varied in key before it is mapped in 3321 binary code .

Figure 5 shows analysis of Avalanche Effect due to one bit change in plaintext when key is constant .It is clear from figure that maximum Avalanche Effect can be obtained when encryption key was kept constant in 8421 binary code(key mapped in 8421 binary code) and data are mapped in 8421 binary code.

Figure 6 shows analysis of Avalanche Effect due to one bit change in encryption key when plaintext is constant .It is clear from figure 5 that maximum Avalanche Effect can be obtained when plaintext was kept constant in gray code (data is mapped in gray code) and data is mapped in 3321 binary code.

Figure 7 shows comparison between avalanche effect of AES and Proposed Algorithm. After evaluating the performance of proposed algorithm we got maximum avalanche effect of 81(out of 128 bit) due to one bit variation in plaintext, when plaintext and key both are mapped in 8421 binary code. We got maximum Avalanche effect of 77(out of 128 bits) due to one bit variation in encryption key (keeping plaintext constant) when plaintext is mapped in Gray and key is mapped in 3321 binary code. But due to property of 3321 code some of the code may be duplicated. Therefore this mapping is not suggested as some code (duplicated code) may be decoded wrongly. Therefore, if one desires a good avalanche effect; AES is a good option.

VII. Conclusion

In this paper a slight enhancement in AES algorithm is proposed. In the proposed algorithm, we have mapped input plaintext and encryption key into various binary codes instead of giving plaintext and encryption key directly to the AES algorithm. The performance of proposed algorithm is evaluated using Avalanche Effect due to one bit variation in plaintext(before being mapped in various binary codes) keeping encryption key constant in a binary code and Avalanche Effect due to one bit variation in encryption key(before being mapped in various binary codes) keeping plaintext constant in a binary code. This leads significant increase in Avalanche Effect of AES Algorithm. Our future work will include experiments on image and focus will be to increase security level.

Acknowledgment

This paper is a part of our M.E. project. I am grateful to my project guide for valuable suggestions, comments and contribution.

REFERENCES

[1] P.Karthigaikumar, Soumiya Rasheed"Simulation of Image Encryption using AES Algorithm" *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011*

[2] Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader,Mohiy Mohamed Hadhoud, "*Evalution the Performance of Symmetric Encryption Algorithms*", international journal of network security vol.10,No.3,pp,216-222,May 2010.

[3] Nidhi Singhal, J.P.S.Raina "*Comparative Analysis of AES and RC4 Algorithms for Better Utilization*" International Journal of Computer Trends and Technology- July to Aug Issue 2011.

[4] Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari "*Performance Evaluation of Cryptographic Algorithms:DES and AES*" IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), March 2012

[5] William Stalling "*Cryptography and network security*" Pearson education, 2nd Edition.

[6] Advanced Encryption Standard Announced by the Federal Information Processing Standards Publication 197, 2001 November 26

[7] A.Anand Kumar,"*Fundamentals of Digital Circuits*", PHI Learning Pvt.Ltd. 2nd Edition

[8] Himani Agrawal and Monisha Sharma "*Implementation and analysis of various symmetric cryptosystems* "Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010)

[9] Sriram Ramanujam,Marimutha Karuppiah"*Designing an algorithm with high avalanche effect*" International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[10] A.Nadeem, "*A performance comparison of data encryption algorithms*", IEEE information and communication technologies, pp.84-89, 2006.Bn

[11] NeetuSettia."*Cryptanalysis of modern Cryptography Algorithms*". International Journal of Computer Science and Technology. December 2010.

[12] Diaasalama, Abdul kader, Mohiy Hadhoud, "*Studying the Effect of Most Common Encryption Algorithms*", International Arab Journal of e-technology, Vol 2, No.1, January 2011.

[13] Ahmed Bashir Abugharsa,Abd Samad Bin Hasan Basari,Hamid Almangush "*A new encryption approach Using the integration of a shifting Technique and the AES algorithm*" International Journal of Computer Application,Volume 42-No.9 March 2012

Chandra Prakash Dewangan received his B.Sc. degrees in Electronics from Pt. Ravi Shankar Shukla University, Raipur in 2004 and completed M.Sc. degrees in Electronics from S.O.S. in Electronics,Pt. Ravi Shankar Shukla University, Raipur, India, and 2006. He is pursuing his M.E. degree at Chhattisgarh Swami Vivekanand Technical University, Bhilai. His area of research includes cryptography and network security.

Prof. Shashikant Agrawal received his B.E degree in Electronics and Telecommunication from Pt. Ravi Shankar Shukla University, Raipur, in 2007 and completed his post graduation from Swami Vivekananda Technical University, Bhilai in 2011. He is currently serving as Assistant professor in the department of Electronics and Telecommunication, Chhatrapati Shivaji Institute of Technology, Durg. His areas of interest include image processing and Information Security He is a life member of Indian Society for Technical Education