Journal of
Information Technology & Software Engineering

Singh, J Inform Tech Softw Eng 2015, 5:1
DOI: 10.4172/2165-7866.1000143

Research Article Open Access

A New Approach to Enhance Avalanche Effect in Aes to Improve Computer Security

Ajeet Singh*

Lecturer in Jagaran Lakecity University, SOET, Bhopal

Abstract

Cryptography is the technique or process by which information or message is sent by a person or users to other person or users so that only the authorized person or users can receive the message. In this research, an Enhanced Advanced Encryption Standard (E-AES) algorithm is proposed for transfer of data to achieve various security goals. This new algorithm is based on the symmetric key encryption Advanced Encryption Standard (AES). E-AES analyzes Advanced Encryption Standard (AES) in terms of security which is calculated by avalanche effect and subsequent memory requirement. It adds one more step by including logical XOR in the existing AES algorithm which ensures improvement in the encryption in terms of 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. The implementation of both techniques has been realized for experimental purposes. Experimental results reflect that E-AES exhibits significant high Avalanche Effect after comparative study with existing encryption algorithm.

Keyword: Encryption; Decryption; Security; Algorithm; Internet: Code; Cryptography

Introduction

Overview

It is already known that the use of internet in this era is increasing very rapidly and many of the users are sharing public and personal information over internet. This gives rise to the need of security as the data and information is very sensitive as its transmission is needed all the time. Encryption technique is one of the key measures which can be very useful to secure confidential information. This encryption is implemented by using some traditional encryption techniques. But traditional encryption technique has some shortcomings in terms of security. This is why an Enhanced encryption algorithm is proposed in this dissertation. This Enhanced encryption algorithm has capacity to improve transmission security, through researching, improving, and arranging several famous data encryption algorithms in some order like Advance Encryption Standard (AES). In this, a new enhanced AES crypto [1-4] concept is proposed by analyzing the principle of the cryptography technique based on the symmetric cryptography function. Moreover, the security and performance of the proposed technique will also be estimated. One function is added in the proposed work that user can directly send encrypted information to another user through email functionality so that security can be increased, rather than encrypting it through another algorithm and then send this information from software. The experimental results based on this symmetric function will approve the effectiveness of the proposed technique, and the enhancement of existing AES will show high-level security. The cipher text generated by this method will be approximately same in size as the plaintext and will be suitable for practical use in the secure transmission of confidential information over the Internet. Basically Cryptography provides a way where we can communicate securely in adversarial environments. Cryptographic technique/method can be symmetric, if both the sender side user and the receiver side user of a information are using the same private/secrete key, as in the case of stream and block ciphers and message authentication codes. Hash functions are also another type of symmetric cryptography technique, where neither sender side user nor receiver side user need to know a private/secrete key at all. In contrast to this, cryptographic technique/method can be asymmetric, if sender side user and receiver side user are using different keys (Public and Private) [4]. Symmetric cryptography technique are very efficient in practically than asymmetric cryptography technique, most security applications use symmetric cryptography to ensure the privacy/confidentiality, the integrity and the authenticity of sensitive/secured data. Even most applications of such type cryptography are actually working in a hybrid manner by transmitting a cipher key with asymmetric techniques while symmetrically encrypting the payload data under the cipher key [5,6]. A cryptosystem is an algorithm or some predefine steps, which include all possible plaintexts/characters, cipher texts, and keys value. Encryption/decryption functions are represented as:

$$E_{Key}(Msg) = Cip$$

$$D_{Key}(Cip) = Msg$$

These functions have the property that:

$$D_{Key}(E_{Key}(Msg)) = Msg$$

Most often, to keep secrets Aes is used for being confidential [6]. Everyone has a need to keep some things secret or confidential. The operating system has secrets or confidential it needs to keep away from users, Many users want their credit card details kept with full secure and away from hackers or attacker, everyone wants their financial and health affairs should be confidential or secret, and, sadly, it appears that even today users still need and required to keep their religious persuasions secret or confidential. It is unfortunate, but the need to keep/secure a wide variety of information secret/confidentially also means that users can also use encryption/decryption to keep secret things that society has decided are unlawful, such as the plans to rob a bank. Encryption/decryption technologies also have other valuable capabilities. Any attempt to falsify the content/information of an encrypted message will cause failure during attempt of decryption. Basically there are three type of cryptography (Figure 1) [7].

***Corresponding author:** Ajeet Singh, Lecturer in Jagaran Lakecity University, SOET, Bhopal, Madhya Pradesh India, Tel: +91 7553040700; E-mail: ajitsingh17985@gmail.com

Received February 22, 2015; **Accepted** April 02, 2015; **Published** April 12, 2015

Citation: Singh A (2015) A New Approach to Enhance Avalanche Effect in Aes to Improve Computer Security. J Inform Tech Softw Eng 5: 143. doi: 10.4172/2165-7866.1000143

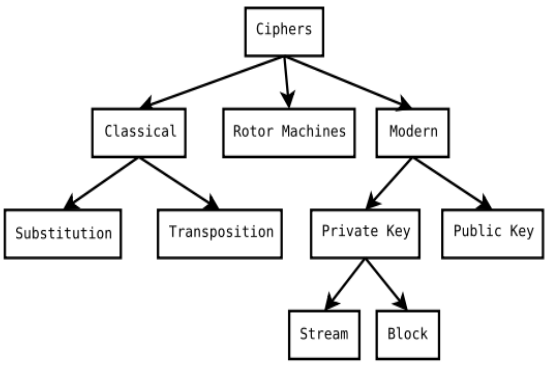

Figure 1: Cryptography Technique Classification.

- Classical cryptography
- Rotor Machine
- Modern Cryptography

In the proposed work we have concentrate on various binary codes, that mean plain text and corresponding key will convert in the selected binary code for the encryption [8,9]. At initial level we have describing existing AES algorithm shown in Figure 2 in brief. The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three steps or stages. This applies for both encryption as well as 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 [10]:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage or step. The 1st nine rounds of the decryption algorithm or technique consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the 10th round simply leaves out the Inverse Mix Columns stage [10]

Rest of the paper is organized as follow: section-II presents proposed work; Section-III presents results analysis and finally section four presents conclusion and references.

Proposed Work

Proposed architecture

Here an enhanced encryption algorithm for transfer of data is presented to achieve the various security goals i.e., Integrity, Availability, and Confidentiality. This new algorithm is based on the symmetric key encryption approach like AES. In this we analyze the Advanced Encryption Standard (AES), and add one more step which is including logical XOR operation to AES to ensure improving the encryption security in terms of avalanche effect. In the proposed algorithm we have applied post processing to standard AES Algorithm to increase the avalanche Effect Figure 3 is showing general block diagram of E-AES. Here plain text and key both are converted into binary code. Then enhanced AES algorithm starts working for encryption which will finally produce cipher text. Detailed architecture is shown in Figure 3. In this all the steps are same except the last step which can be defined as:

• Take produced cipher text from AES and convert it into binary form. Then the output (128×N) bits of AES algorithm is produced as cipher text and is arranged in following way

B1	B2	B3	B4	B5	B6	B7	B8	…	Bn

Then apply XOR operation between each bit together. The last bit will be XOR with first bit.

For Example, B1 = B1 *EXOR* B2, B2 = B2 *EXOR* B3, Similarly, Bi = B (i) *EXOR* B (i+1), in decryption reverse processing of above steps takes place.

Results

For experiment purpose, proposed system has implemented AES

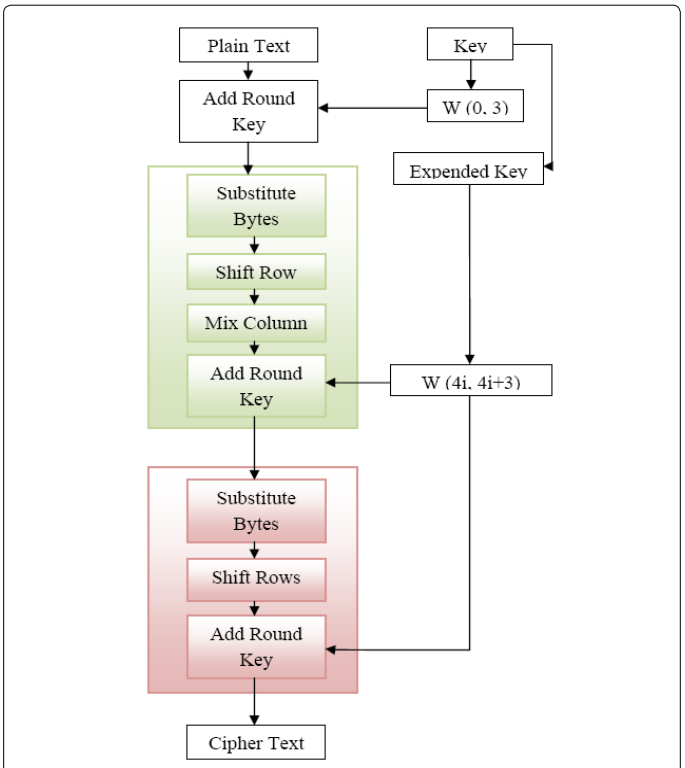

Figure 2: AES Architecture

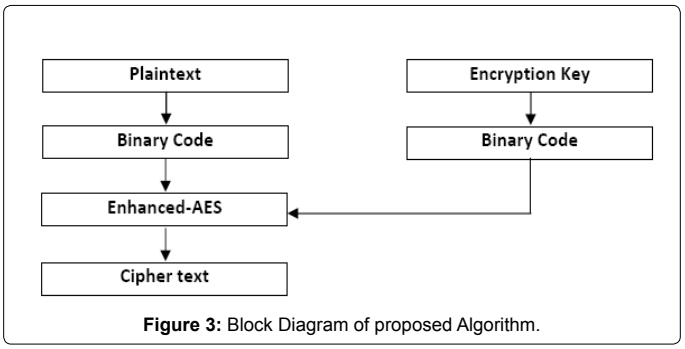

Figure 3: Block Diagram of proposed Algorithm.

and modify AES algorithm. Architecture of AES as shown in Figure 2 and modify AES architecture shown in Figure 4. Figures 2 and 4 has one step difference which is binary bit conversion with logical XOR operation in Figure 4. At the time of results calculation a desktop machine are using and the configuration of that machine is Intel Pentium Dual Core E3400 3.61 Ghz, 1 GB of RAM and Window-XP, in which performance data is collected. In the experiments, the system encrypts/decrypt with various binary code on various combinations of test message and filliped message. Each time, different plaintexts are respectively encrypted by AES and E-AES. Finally, the outputs of AES and E-AES are compared with each other in terms of avalanche effect, and it is measured in numeric form. Actually, for an encryption algorithm, the avalanche effect of encryption not only depends on the algorithm's complexity, but also the key and the plaintext have certain impact. Table 1 is demonstrates comparison between avalanche effect of AES and E-AES. In this table alphabets are converted into binary codes of seven types and then alphabet 'J' is flipped with alphabet 'A'. Here it can be seen that in each scenario of binary code, the avalanche effect of proposed algorithm is always greater than the existing AES. But highest avalanche effect in proposed algorithm is 75 which are achieved with binary code 5311 and second highest value is 67 with Gray binary code. It seems that both these binary codes will give us the desired result in terms of avalanche effect. The result produced in Table 1 is been graphicaly represented in Figure 5. It is clearly shown that result of avalanche effect is produced highest with binary code 5311. Moving further in result now in Table 2 alphabets are converted into binary codes of seven types and then alphabet 'A' is flipped with integer '5'. The motive here is to calculate the avalanche effect by flipping of character with integer. Here it can be seen that the binary code 5311 and the gray code that were producing the highest and the second highest result in the above table are now producing only 61 and 62 results respectively. Also the difference between the results of AES and E-AES is negligible that is one. Hence it can be concluded that the flipping of character with integer is not fruitful to achieve the target. But the surprising element is that the highest result produced in binary code 3321 is 77 which is not only highest in this table but is also higher than any other value produced in Table 1. In the same binary code i.e 3321 the difference between avalanche effect of AES and E-AES is 24 which is quite noticeable and therefore the research can be carried out in consideration with binary code 3321. The result produced in Table 2 is been graphically represented in Figure 6. So it can be concluded by above research that code 3321 is highly considerable. Now one of the characters in test sentence 'This is India', character 'd' is flipped one by one with integers ranging from 1 to 9. Maximum avalanche effect can be seen by flipping 'd' with integer '3' that is 228. Here the difference between AES and E-AES is maximum that is 38. From the Table 3 it can be seen that minimum difference from AES is 21 and it ranges up to 38. This is quite significant and noticeable. Result of Table 3 is graphically represented in below Figure 7. It clearly shows that the difference of avalanche effect between AES and E-AES is significant. The above discussion concludes that by using proposed algorithm that is E-AES we get maximum avalanche effect when plain text is firstly converted into 3321 binary code and any character in plain text is flipped by integer value. It is clear from Table 3, E-AES can produce avalanche effect above 200 with all possibility but flipping of character with special symbol is quite not acceptable because it can create confusion after decryption. On other hand flipping of character with integer is quite acceptable. For example we can write '0' zero as 'o' and '1' one as 'l'. In this type of flipping we also get significant avalanche effect.

Conclusion

In this dissertation enhancement in AES algorithm is proposed. In the proposed algorithm that is E-AES, input plaintext and encryption key are mapped into various binary codes instead of giving plaintext and encryption key directly to the AES algorithm. E-AES includes two more steps to AES, which converts plain text into binary with logical and strong XOR operation. E-AES performs better when compared with the existing AES this is reflected by the corresponding is Avalanche Effect of both the existing and proposed E-AES due to one bit variation in plaintext (before being mapped in various binary codes) keeping encryption key constant in a binary code. Results and Analysis section indicates that the E-AES is definitely comparable with AES. The performance of E-AES is significantly better than AES algorithm. This result is achieved because the cipher produced by E-AES has strong bit level dependence. By result and analysis section it can be also concluded that E-AES can produce cipher with high avalanche effect in any binary code conversion as compared to AES.

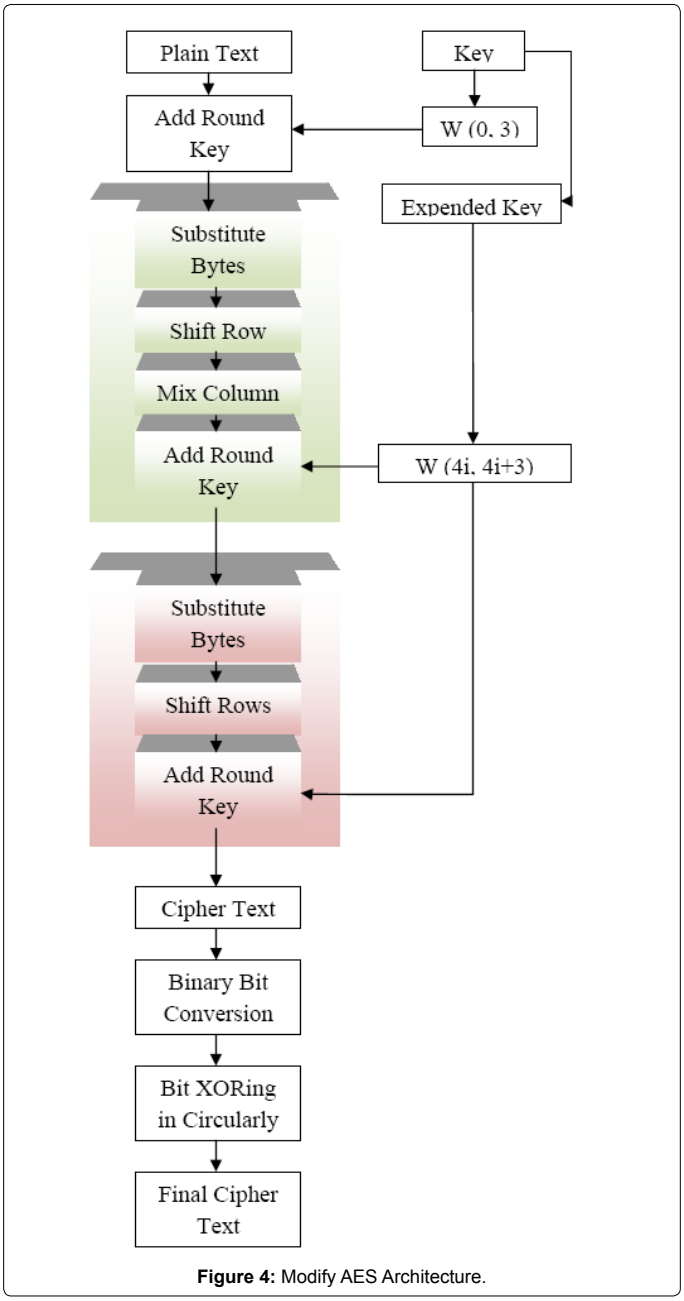

Figure 4: Modify AES Architecture.

CODE	STRING	C STRING	NUMBER OF BITS FLIPPED WITH AES	NUMBER OF BITS FLIPPED WITH E-AES	AVALANCHE % OF AES	AVALANCHE % OF E-AES	DIFFERENCE OF FLIPPED BITS (AES AND E-AES)
Gray Code	**J**	**A**	**50**	**67**	**39.1**	**52.34**	**17**
8421	**J**	**A**	**56**	**66**	**43.8**	**51.56**	**10**
7421	**J**	**A**	**60**	**63**	**46.9**	**49.22**	**3**
5421	**J**	**A**	**62**	**62**	**48.4**	**48.44**	**0**
5311	**J**	**A**	**61**	**75**	**47.7**	**58.59**	**14**
5211	**J**	**A**	**65**	**65**	**50.8**	**50.8**	**0**
4221	**J**	**A**	**58**	**60**	**45.3**	**46.88**	**2**
3321	**J**	**A**	**57**	**64**	**44.5**	**50**	**7**

Table 1: Avalanche effect comparison between AES and E-AES.

CODE	STRING	C STRING	NUMBER OF BITS FLIPPED WITH AES	NUMBER OF BITS FLIPPED WITH E-AES	AVALANCHE % OF AES	AVALANCHE % OF E-AES	DIFFERENCE OF FLIPPED BITS (AES AND E-AES)
Gray Code	A	5	61	62	47.7	48.4	1
8421	A	5	60	61	46.9	47.7	1
7421	A	5	61	65	47.7	50.8	4
5421	A	5	58	63	45.3	49.2	5
5311	A	5	62	63	48.4	49.2	1
5211	A	5	54	61	42.2	47.7	7
4221	A	5	66	68	51.6	53.1	2
3321	A	5	53	77	41.4	60.2	24

Table 2: Avalanche effect comparison between character and numeric by AES and E-AES.

S.NO	3321 CODE	ORIGINAL STRING	CHANGED STRING	BITS IN CIPHER TEXT	NUMBER OF BITS FLIPPED WITH AES	NUMBER OF BITS FLIPPED WITH E-AES	DIFFERENCE OF FLIPPED BITS (AES AND E-AES)
1	3321 Code	This is India	This is In1ia	1152	186	210	24
2	3321 Code	This is India	This is In2ia	1152	182	214	32
3	3321 Code	This is India	This is In3ia	1152	190	228	38
4	3321 Code	This is India	This is In4ia	1152	184	210	26
5	3321 Code	This is India	This is In5ia	1152	187	208	21
6	3321 Code	This is India	This is In6ia	1152	182	220	38
7	3321 Code	This is India	This is In7ia	1152	180	210	30
8	3321 Code	This is India	This is In8ia	1152	181	218	37
9	3321 Code	This is India	This is In9ia	1152	188	216	28

Table 3: Result and Comparison of Avalanche Effect in a Sentence with 3321 code where character is flipped by Integer.

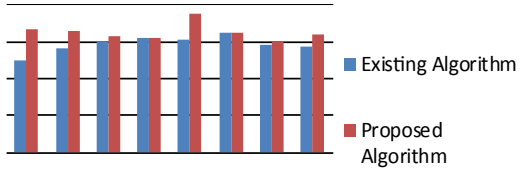

Figure 5: Avalanche effect Comparision between AES and E-Aesanche.

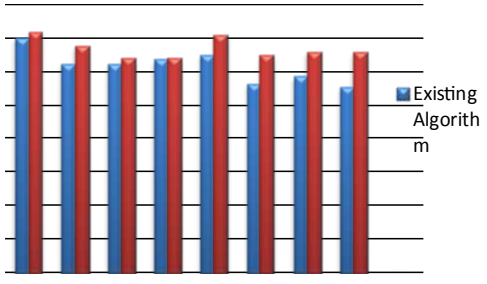

Figure 6: Avalanche Effect Comparison Between character and numeric by AES and E-AES.

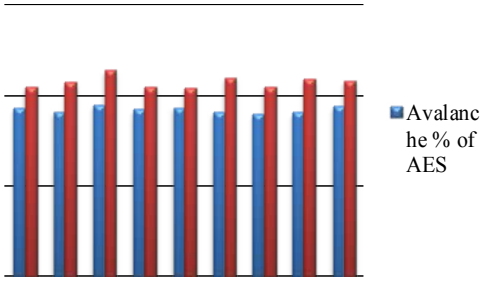

Figure 7: Result and Comparison of Avalanche Effect in a Sentence with 3321 code where Character is flipped by Integer.

Application

Enhanced AES algorithm can be applied in various systems like banking, defense, finance, government, educational, medical science and many more where confidential data are being stored in large manner and is being used in public network.

Limitation

Proposed algorithm is an enhancement to the AES algorithm so

cryptanalysis is dependent on the AES architecture. If any dispense is found in AES then it will also reflect on proposed algorithm.

Future enhancement

In this dissertation algorithm used is E-AES works on post processing on cipher text generated by AES by which we achieve strong bit level dependence and improved avalanche effect. In future researches E-AES can be modified with both pre and post processing on AES to enhance security and efficiency of transmitting data.

References

1. Dewangan CP, Agrawal S, Mandal AK , Tiwari A (2012) Study of Avalanche Effect in AES Using Binary Codes. International Conference on Advanced Communication Control and Computing Technologies.
2. Mandal JK, Paul M (2012) A Bit Level Session Based Encryption Technique to Enhance Information Security. International Journal on Computer Science and Engineering 4: 321-326.
3. Landge I, Burhanuddin C, Patel A, Choudhary R (2012) Image encryption and decryption using blowfish algorithm.World Journal of Science and Technology 2: 151-156.
4. Prakash C, Dewangan, Agrawal S (2012) A Novel Approach to Improve Avalanche Effect of AES Algorithm. International Journal of Advanced Research in Computer Engineering & Technology 1: 248-252.
5. Sastry VUK, Murthy DSR, Bhavani SD (2010) A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side. International Journal of Computer Theory and Engineering 2: 805-808.
6. Mohit K, Mishra R, Pandey RK, Poonam Singh (2010) Comparing Classical Encryption With Modern Techniques 1: 49-54.
7. Sastry UV, Shanker NV, Bhavani SD (2009) A modified Playfair Cipher Involving Interweaving and Iteration International journal of Computer theory and Engineering 5: 597-601.
8. Elminaam DSA, Kader HMA, Hadhoud MM (2010) Evaluating the Performance of Symmetric Encryption Algorithms. International journal of network security 10: 216-222.
9. Hashim AT (2010) FPGA Simulation of Type-3 Feistel Network of The 128 bits Block Size Improved Blow fish Cryptographic Encryption. Eng & Tech .Journal 28: 115-119.
10. Landge IF (2011) Implementation of AES Encryption & Decryption using VHDL. International J of Engg. Research & Indu Appls 4: 395-406.