International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 09 | Sep -2017 www.irjet.net p-ISSN: 2395-0072

Performance Analysis of Application for Security Enhancements using Cryptanalysis

Malvina Rumao[1], Vikas Kaul[2], Deven Shah[3], Dr S K Narayankhedkar[4]

[1] *P.G Student, Thakur College Of Engineering and Technology / Mumbai University, India*
[2] *Asst. Prof, Thakur College Of Engineering and Technology / Mumbai University, India*
[3] *Professor, Thakur College Of Engineering and Technology / Mumbai University, India*
[4] *Professor, MGMCOET, Navi Mumbai*

Abstract - *With advent of new technologies, enormous amount of applications flow through the internet making it critical to handle the security aspects of data in the applications.Advanced Encryption standards coupled with many such security algorithms and its various versions are used to increase confidentiality and provide integrity of data. Also due to advancement in attacks, security algorithms have become vulnerable to various kinds of cryptanalytic attacks. The most important constituent of symmetric cryptosystem is Substitution box as it enhances security of cryptography by providing non-linearity.*

Dynamic S-box is designed so that S-box is changed in every round based on key and number of rounds by using RC4 algorithm, and complexity is enhanced by using round structure thus increasing the level of difficulty for attacker. Performance evaluation of the above system is done on randomness test which includes strict avalanche criteria, Differential approximation probability and linear approximation probability. Cryptographic properties are evaluated by using this software which will help to determine the quality of S-box thus analyzing AES.

Key Words: Cryptography, Advanced Encryption Standard, Strict Avalanche Criteria, Linear Cryptanalysis, Differential Cryptanalysis

1. INTRODUCTION

Important concern in developing efficient communication is providing Data security. Effective method of cryptography is adopted to solve this issue effectively to provide integrity, availability, authentication, privacy, accuracy and computability. Cryptography means secret writing which uniquely define the mathematical steps required to encrypt and decrypt messages in a cryptographic system, thus protecting data from unauthorized access [1].The mathematical procedure of encipherment enriches cryptographic products, e-trading, e-banking, e-commerce and electronic signatures for secure transactions. Encipherment process transforms plain text to the scrambled cipher text To offer secure transmission and storage of information/data, many symmetric algorithms were proposed such as Data Encryption Standard (DES), the Elliptic Curve Cryptography (ECC), Rijndael Algorithm and etc. Cryptography is science of encryption and decryption of confidential and often sensitive messages [3]. The Advanced Encryption Standard algorithm (AES) has been defined by National Institute of Standards and technology of United States as a new private key decryption algorithm. AES algorithm on the basis of attributes: encipherment and decipherment and degree of security issues essential for safe wired and wireless communication [4]

1.1 Advanced Encryption Standard

The Advanced Encryption Standard(AES) was designed because DES's key was too small and triple DES was a slow process. The National Institute of Standard and Technology(NIST) chose the Rijndael algorithm named after its Belgian Inventors, Vincent Rijmen and Joan Daemen. AES is very complex round cipher. Number of rounds in AES depends on Key size: key size of 128 bits-number of rounds is 10, key size of 192 bits-number of rounds is 12, key size of 256 bits-number of rounds is 14. An Encryption system contains set of transformation that converts plain text to cipher text, these set of transformation are Shift row transformation, Mix column transformation, Add round key and sub-byte transformation. Fault attacks on AES can be classified into two categories depending on fault location: fault attack on key schedule and fault attack on encryption process.

1.2 AES S-Box

Same S-box used in every round is being referred to as Static S-box while key dependent S-box means that S-box changes in every round depending on the number of keys and number of rounds. By making S-box key dependent we assume S-box will be strong. The round key generated will be used for finding a value that is use to rotate S-box[5].

1.3 RC4

A algorithm designed by Rivest for RSA data security named RC4 is a variable key-size stream cipher with byte oriented operations. This algorithm is used for random permutation.RC4 is file encryption algorithm to establish secure communication[6].

2. Literature Review

The below literature survey analyzes the work done by array of researchers and scholars in field of data and network security. The technical papers stated below gives the idea of performing analysis of application for security enhancement using cryptanalysis.

In paper [1], authors Nan Lio, Xiaoxin Cui, Tang Wang, Kai Liao and Dunshan Yu have proposed a method to overcome faults in S-box by proposing Fault model based on S-box faults in encryption process. Two models have been proposed aiming at S-box faults in round 10th round and 9th round encryption process

In paper [2], the authors Shivlal Mewada, Pradeep Sharma, S.S Gautam explores efficient private key algorithm based on security of individual system and to improve encipherment and Decipherment time with encipherment/Decipherment performance.

In paper[3],Ashwak Alabaichi, Adnan Ibrahem Salih, discusses the enhancement of the AES algorithm and describes the process, which involves the generation of dynamic S-boxes for Advance Encryption Standard(AES) values of correlation confection for dynamic AES and AES
In paper[4], authors Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman state that the original S-box consists of 4 stages while in this new design, it consists of five stages, the extra stage is known as S-box rotation and it is introduced at beginning of round function. It shows very strong resistance against linear cryptanalysis and differential cryptanalysis. In paper [5],authors summarize Yong Wang, Qing Xie, Yuntao Wu, Bing Du, the performance index and are analyzed. Software for testing performance index of S-box is developed through which evaluation is done to find high cryptographic performance.

In paper [6],authors Ripal Patel and Vikas Kaul have enhanced AES using RC4 algorithm to create dynamic s-box and key scheduling algorithm to increase its complexity.

3. Proposed System

Security of whole cryptography system is based of security of S-box. Evaluation of security of S-box and design issues in S-box is still of concern in block cipher. Static S-box are vulnerable to various types of attacks, so by using dynamic S-box it is difficult for attackers to do any offline interpretation of particular set of S-box. The goal of this project is to evaluate the effect of dynamic S-box on security of AES. These S-boxes can be created when they are required and thus reduce the need of storing large data structures within algorithm. Performance indexes will help in determining the cryptanalysis of the generated S-box so that it can be evaluated for its security enhancement. System can be made more complex by using AES round structure. SHA-256 is use to provide integrity of data and RSA is used as key exchange algorithm. Performance evaluation of the above system is based on randomness test which includes Strict avalanche criteria, Differential approximation probability and Linear approximation probability.

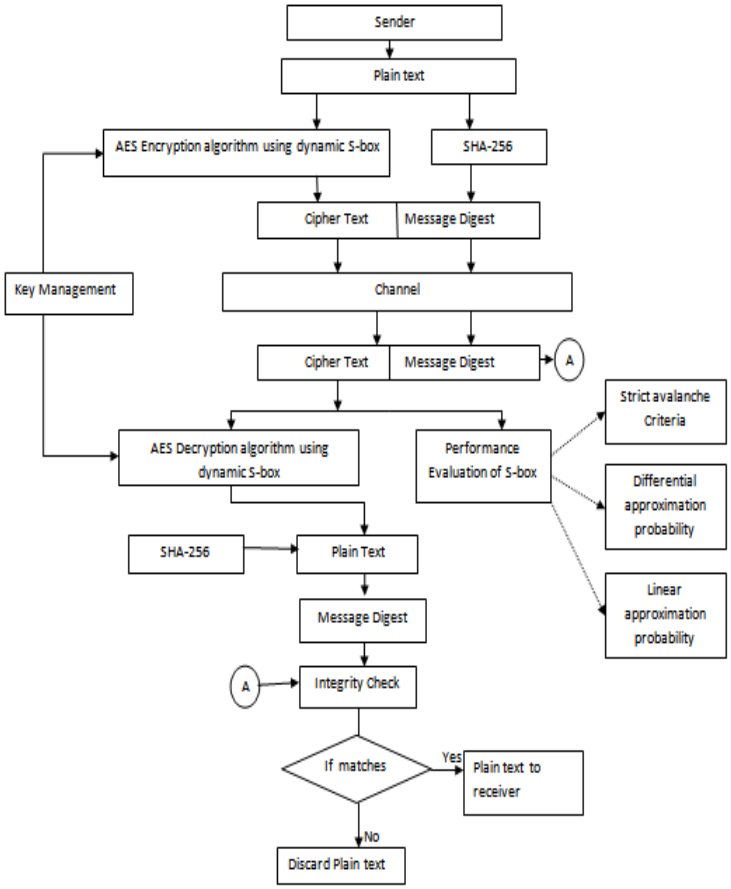

Fig 1: Proposed System

4 . Design Methodology

The proposed dynamic S-box has the same block length and key length as the original AES. It has block length which is 128 bits and three key lengths which are 128, 192, and 256 bits. The dynamic AES includes two processes, which are encryption and decryption. These processes resemble the original AES with an additional step that is introduced at the start of the round function. This step is called S-box Permutation, below figure illustrate the proposed dynamic AES. It is noticed that the last four stages are the same as those in the AES[1].

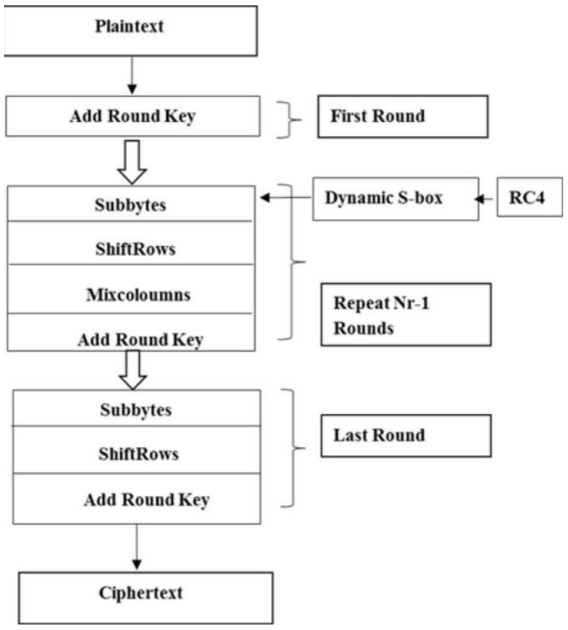

Fig 2: AES Dynamic S-box

The Key expansion transformation takes key and generates expanded key and output of key pseudo expansion algorithm i.e expanded key is used to generate S-box by RC4 key schedule algorithm to prevent repetitions.

To increase complexity, round structure is used which takes input of 256 bits which is divided in two blocks of 128 bits each. One block of 128 bits is given as input to AES section of system and other block of 128 bits is given to AES section of system in next round as per structure. Process is continued as per the rounds suggested. The output is constructed by combining all the data together.

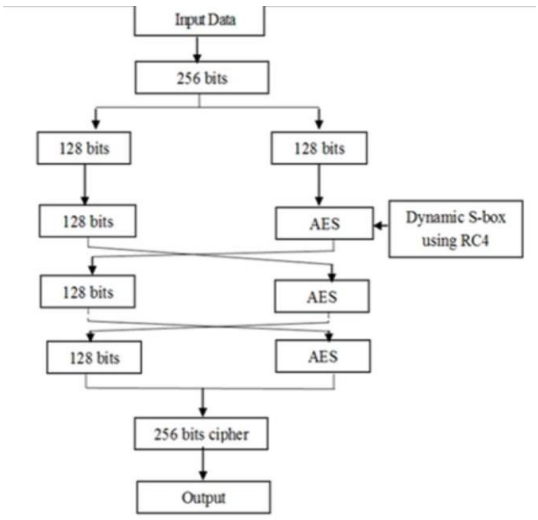

Fig 3: AES in Round Structure

Performance Evaluation:

1. Strict Avalanche Criteria:

In Strict avalanche criteria we look at each bit one by one and verify that whatever the other bits will change it will have a 50% probability to switch. Each bit should have 50% chances to change if you change 1 bit of input. It is satisfied if, whenever a single input bit is complemented each of its bits changes with a 50% probability. Strict avalanche criteria consists of absolute indicator and sum of square indicator. It is calculated by stating absolute indicator value and value of sum of square indicator.

2. Linear Approximation Probability.

High probability occurrence of linear expression involving plaintext bits and cipher text bits. The resistance of S-box to Linear cryptanalysis is closely related to co-efficient of Walsh Hadamard Transform of all non-zero linear combination of relevant component function, it is use to calculate nonlinearity, bigger the nonlinearity unsuccessful is the attack. Linear Cryptanalysis is to find an approximate of relationship between plain text, cipher text and key, i.e presenting linear dependence involving three parties.

3. Differential approximation Probability.

The differential approximation probability is based on analysis of effect of particular differences in plain text and on the differences of resultant cipher text pairs. These differences are use to assign probabilities to possible keys in cipher text and locate the most probable key. If differential delta uniformity(DDT) is flatter than the probabilities for distinct differences are similar and no information can be extracted. The attacker computes the differences of corresponding cipher text hoping to detect statistical pattern in their distribution with help of XOR operation, one particular cipher text difference is expected to be especially frequent in this way cipher can be distinguished from random text.

5 . Results

File: “plaintext.txt”, Size: 144 bytes (1552 bits), Key: 12345678901234561234567890123456

Table -1: Encryption time and Decryption time is recorded using text file as input on Microsoft Windows 10, Intel i3, 64 bit, 6 GB RAM

Sr. No	Algorithm	Block size	Encryption Time (Sec)	Decryption Time(Sec)
			i3	i3
1	AES	128	0.00252	0.00323
2	Enhanced AES	128	0.00291	0.00348
3	Round Structure (1R)	256	0.00275	0.00317
4	Round structure with Enhanced AES(1R)	256	0.00299	0.00359
5	Round structure (5R)	256	0.00290	0.00337
6	Round structure with Enhanced AES(5R)	256	0.00337	0.00435
7	Round Structure (10R)	256	0.003283	0.00356
8	Round structure with Enhanced AES (10R)	256	0.00389	0.00480

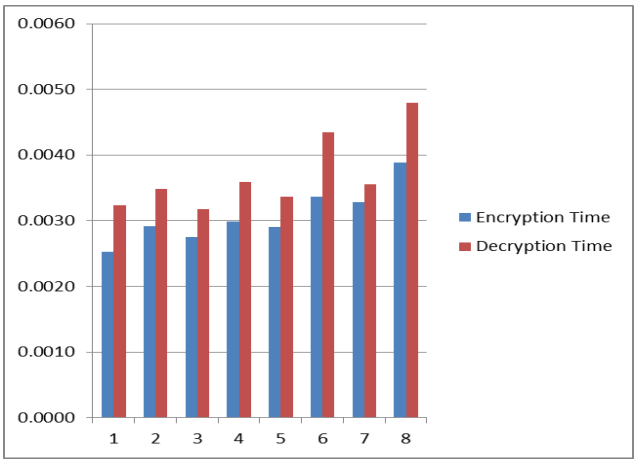

Fig 4: Graphical Representation for encryption time and decryption time for text input

File: "img.png", Size: 144 bytes (1552 bits), Key: 12345678901234561234567890123456

Table -2: Encryption time and Decryption time is recorded using image file as input on Microsoft Windows 10,Intel i3, 64 bit, 6 GB RAM

.Sr. No	Algorithm	Block size	Encryption Time (Sec)	Decryption Time(Sec)
			i3	i3
1	AES	128	0.02332	0.02378
2	Enhanced AES	128	0.02502	0.03160
3	Round Structure (1R)	256	0.01653	0.01687
4	Round structure with Enhanced AES(1R)	256	0.016443	0.0176
5	Round		0.05820	0.061371

	structure with Enhanced AES(5R)	256		
6	Round structure with Enhanced AES(5R)	256	0.0595	0.06323
7	Round Structure (10R)	256	0.11268	0.13308
8	Round structure with Enhanced AES (10R)	256	0.11386	0.11932

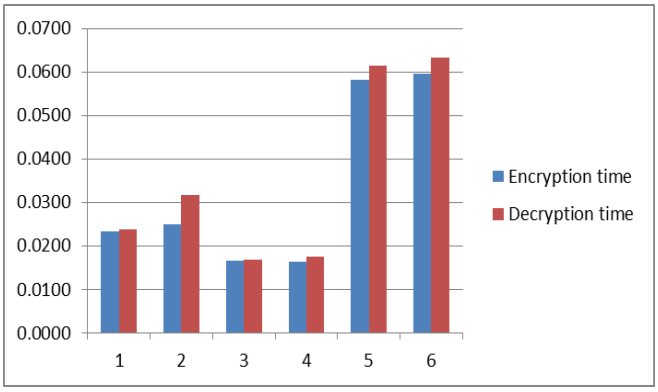

Fig 5: Graphical Representation for encryption time and decryption time for image input

Performance Analysis is done by using strict avalanche criteria, Linear approximation probability and Differential approximation probability. Strict Avalanche criteria is calculated using absolute indicator and sum of square of indicator. The smaller is the value of absolute indicator and sum of square indicator the better is Strict avalanche criteria. Linear approximation probability is obtained by calculating Nonlinearity, greater the value of nonlinearity unsuccessful is the attack. Differential approximation probability is robustness to differential cryptography, hence the value should be high for ideal AES. S-box of Traditional AES and Enhanced AES is given as input and values for nonlinearity, Differential approximation probability and absolute indicator and sum of square of Indicator are obtained.

Table -3: Performance analysis of Traditional AES and Enhanced AES using RC4

Sr.No	Algorithm	Strict Avalanche Criteria	Nonlinearity	Differential Approximation Probability
1	AES	32, 133120 (Absolute indicator:32, Sum of Square of Indicator:133120)	112.0000	0.98
2	Enhanced AES with dynamic S-box using RC4	96,283648 (Absolute indicator:96, Sum of Square of Indicator:283648)	94.000	0.96

6 . Conclusion

Security is key aspect of communication, encryption of information makes it inaccessible to unauthorized recipients. One of the most secure encryption algorithm is AES encryption. Due to increasing use of technology and large amount of data being transferred with not enough security this sensitive data becomes vulnerable to different attacks. Main reasons or vulnerability of AES encryption algorithm is use of static S-boxes. This project proposes a method to make S-box dynamic so that its structure is hidden from cryptanalyst making it difficult for attackers to attack and thus making it resistant to differential and linear cryptanalysis. Performance Index such as Strict avalanche criteria, Differential approximation probability and Linear approximation probability are used to evaluate the performance of AES. It is observed that Enhanced AES with dynamic RC4 resists to linear and differential cryptanalysis and also its Encryption and Decryption time has been recorded using various versions of AES algorithm.

REFERENCES

[1] Nan Liao, Xiaoxin Cui, TiangWang,Kai Liao, DunshanYu"A high- efficient fault attack on AES S-box".

[2] ShivlalMewada, Pradeep Sharma, S. S. Gautam,"Exploration of Efficient Symmetric AES Algorithm ",2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[3] Ashwakalabaichi, Adnan IbrahemSalih, "Enhance Security of Advance EncryptionStandard Algorithm Based on Key-dependent SBox", ISBN: 978-1-4673-6832-2©2015 IEEE

[4] Julia Juremi, RamlanMahmod, SalasiahSulaiman." A Proposal for Improving AES S-box with Rotation and Key- Dependent"

[5] Yong Wang, Qing Xie, Yuntao Wu, Bing Du, "A Software for S-box Performance Analysis and Test", 2009 International Conference on Electronic Commerce and Business Intelligence

[6] Ripal Patel, Vikas Kaul," Security Enhancement in Next Generation network using Enhanced AES with RC4 and dynamic S-box", 2017 Internation Research Journal of engineering and Technology.

[7] Farshid Hossein Nejad, Saman Sabah, Amid Jamshidi Jam," Analysis of Avalanche Effect on Advance Encryption Standard by Using Dynamic S-Box Depends on Rounds Keys. ",International Conference on Computational Science and Technology – 2014 (ICCST'14)

[8] Abhiram.L.S, Gowrav.L, PunithKumar.H.L "Design and synthesis of Dual Key based AES Encryption", MSRIT, BANGALORE, India, 21-22 NOVEMBER 2014.

[9] Thomas Fuhr, Eliane Jaulmes, Victor Lomne and Adrian Thillard "Fault Attacks on AES with faulty Ciphertexts Only" , 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography.

[10] Howard M.Heys,"A Tutorial on Linear and Differential Cryptanalysis".