International Conference on Advanced Computing, Communication and Networks'11

Pattern Evaluation of AES using Monte Carlo Test

Sandeep Mahapatra[1], Rupali Syal[2]

Suraj Kumar Sunar[3], Karanveer Singh[4]

Department of Computer Science and Engineering
PEC, University of Technology

[1]s.mahapatra15101987@gmail.com, [2]rupali@pec.ac.in

[3]surbhu06@gmail.com, [4]karan.shergill892@gmail.com

***Abstract*— Security is the important concern in the area of data communication. Through encryption security has been provided in data communication. Several encryption techniques are available for security where AES (Advance Encryption Standard) is one of the strongest symmetric cipher techniques which is not easy for any attacker to make attack on this technique. To verify that this technique is the strongest one by finding out no similarity in cipher text after encryption process over different type of plaintext likes character, integer, character and integer, special character etc. The AES (Advance Encryption Standard) has been embedded with CBC (Cipher Block Chaining) block cipher mode of operation, which is used to cover virtually all possible applications of encryption then the evaluation has been done through Monte Carlo Test. With the help of this test we accumulate a set of different plaintext and their corresponding cipher text with their key value. We have analysed that the cryptanalysis is not possible on AES (Advance Encryption Standard), it's not possible for attacker to find out the skeleton of the plaintext through the pattern of cipher text. The final analysis gives some better result which verifies that AES is strongest symmetric cipher.**

***Keywords*— Encryption, Decryption, AES, Cryptanalysis, Security, Cipher text, Monte Carlo**

I. INTRODUCTION

In today's world there are many encryption techniques and they mainly concern about the security of data communication. Encryption as well as decryption both is important aspects of security [1], [3]. Sender sends the data which is encrypted with the help of secret key, encrypted message is called cipher text [10] and which is received by the receiver. If this cipher text is captured by other one, it will not be able to understand or use by other one. When receiver receive the cipher text, then again key is use to convert it original plain text. So in this process at the communication line only cipher text consist, which is non sense for the other. Original message resides at the both terminal. So the data is secure while communication.

AES[7] is one of the strongest symmetric cipher technique which is commonly employed at every field. The only requirement of symmetric encryption is secret key which is used to hide the message. Cryptanalysis is commonly used by attacker in order to steal information against the AES technique [7], [8]. Through this attack attacker tries to find out the skeleton of original plain text but the probability to find out original message is very less.

Various types of encryption techniques are available, but the application of them creates difference. When data is more sensitive and cannot be lost at any cost then AES technique is used although the cost of AES algorithm is very high that's why it cannot be implemented everywhere, the complexity of the AES is very high which are explained at next section.

In our experiment we carried out encryption process over AES (Advance Encryption Standard) along with CBC (Cipher Block Chaining) [10] .After that we analysed the plaintext of different data types along with their corresponding cipher text using Monte Carlo Test.

In this paper, next section describes the algorithm of the AES (Advance Encryption Standard) encryption techniques, CBC (Cipher Block Chaining) [10]. Along with that Monte Carlo Test [4] is also discussed which is used for the accumulation of set of plaintext and their corresponding cipher text with their key value. Then third section describes the methodology adopt for the evaluation of the AES in CBC mode through Monte Carlo Test. Fourth section is experimental result and analysis which shows the cumulative result of plaintext , keys and it's corresponding cipher text and the last section conclude the paper.

II. AES, CBC & MONTE CARLO

In this section we will describe the AES (Advance Encryption Standard) encryption techniques and Monte Carlo Test.

A. AES (Advance Encryption Standard)

AES [8], [10] is a symmetric block cipher, proposed by two Belgium cryptographers: - Dr. Joan Daemen and Dr. Vincent Rijmen. It was published in 2001 by NIST.

AES either consist of 10, 12 and 14 rounds and the number of rounds in AES is decided on the basis of size of key. If the size of key is 4, 6 and 8 words then the number of rounds will be 10, 12 and 14 respectively. The size of plaintext is 4 words (128 bits) which is same for all. Each round of AES has these four stages in his round except in an initial and final round.

1. Substitute bytes
2. Shift rows
3. Mix columns
4. Add round key

Our experiment carried over 16 bytes key and 16 bytes plaintext, so AES has 10 rounds as we mentioned. In AES before first round, plaintext has to enter in Add round key process then from round 1 to round 9 plaintext processed through all these 4 stages in every round which mentioned above. Finally at round 10 it has only 3 stages (Substitute bytes, Shift Rows, Add round key). In round 10 mix column stage is omit.

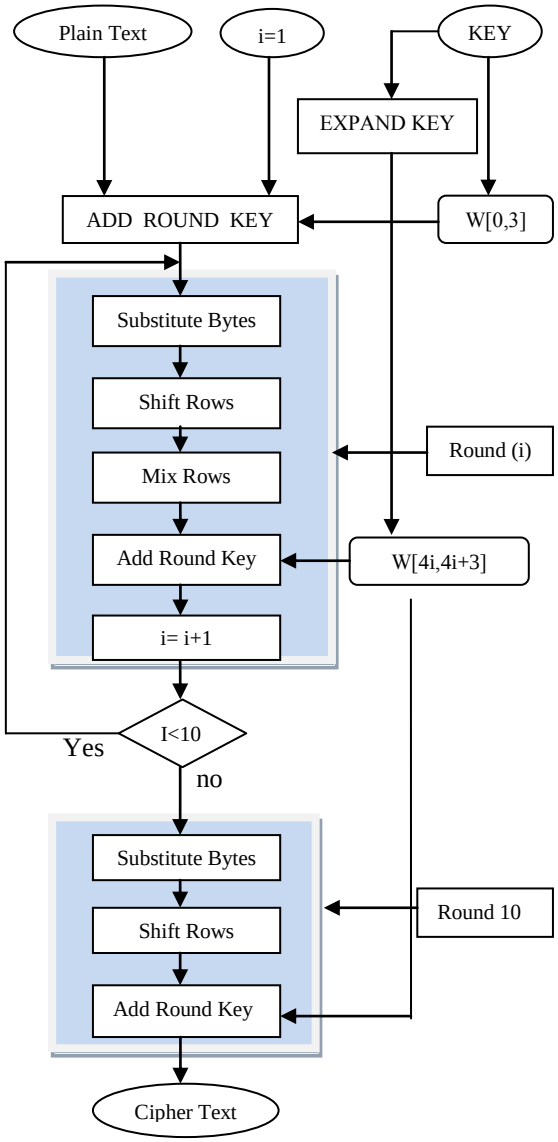

Figure 1: AES (Advance Encryption Standard) Process

B. CBC (Cipher Block Chaining)

There are 5 types of different types of Block cipher modes of operation (ECB, CBC, CFB, OFB, and CTR) [10] .These modes of operation use with any symmetric block cipher.

Basically the CBC [10] is designed to overcome from the problem of security deficiencies of ECB [10]. If the same plaintext block is introduced again then CBC produce the different cipher text block. In the operation of CBC mode, initially the first plaintext block is XOR with the initialization vector (IV) and produce first cipher text block after the first step current plaintext block will XOR with the preceding cipher text block. During process of each and every block of plaintext same key is used. The key and IV (Initialization vector) should be protected from attacker, the IV (Initialization vector) is also important as key.

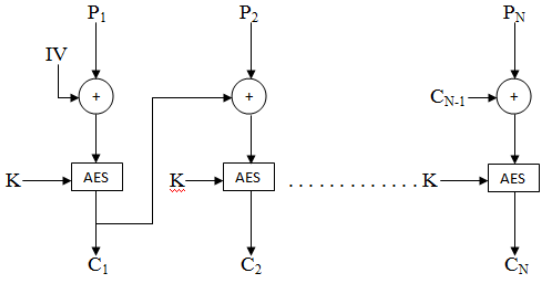

Figure 2: CBC (Cipher Block Chaining)

$$C_1 = E_k (IV \oplus P_1) \quad (1)$$

$$C_n = E_k (C_{n-1} \oplus P_n) \text{ , where n=2,3,4.....} \quad (2)$$

C. Monte Carlo Test

Monte Carlo test is a type of computational algorithm in which random sample has been selected and computes the result of each and every random sample. It is mostly used in mathematical system. Monte Carlo test is very useful in studying any system with large number of random samples and also useful in calculation of risk analysis in business. Monte Carlo Test has large number of applications in engineering it plays a vital role in an analysis of almost every engineering application .In Monte Carlo test the input has been selected randomly and there is very much uncertainty in inputs. With the help of this test it is possible to find out the loop holes of any system or mechanism, through the observation of various results on the basis of random input. These are the following steps involved in Monte Carlo test:-

1. Define a domain of possible inputs
2. Generate inputs randomly from the domain
3. Use these inputs over any operation or computation

4. Aggregate the results of individual computations as a final result.

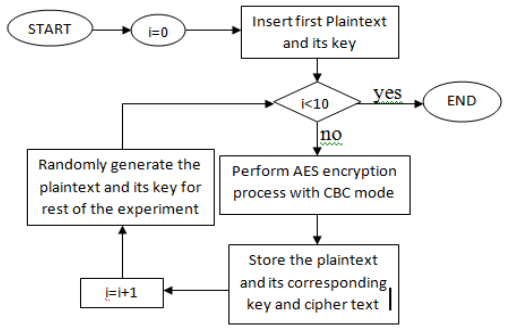

Figure 3: Monte Carlo test on AES with CBC mod

III. Methodology

AES (Advance Encryption Standard), Monte Carlo Test and CBC (Cipher block chaining) are explained in previous section. Consider AES parameter in mind we perform encryption process on AES with CBC mode. We implemented experiment with 16 bytes of plaintext with 16 bytes of key as a result of encryption process 16 bytes of cipher text is also generated.

All encryption techniques are implemented in MATLAB 7.11.0.584 (R2010b), Intel core i3 processor, 2GB RAM 32 bit window 7 operation system. Optimized code is uses for the process and during the experiment only first key and first plaintext has been given by user and for the rest of the experiment their plaintext and keys are generated randomly. By applying Monte Carlo test we accumulate the several random keys and random plaintext along with their cipher text. So that we analyse the pattern of cipher text of various different types of data types.

IV. Experimental Results and Analysis

According to the methodology we have performed the Monte Carlo Test over AES (Advance Encryption Standard) with CBC mode. In our experiment except in our initial stage we randomly generate the plaintext and it's keys and perform the AES encryption process with CBC mode. The domain of the Monte Carlo test varies from 0 to 255. In AES with CBC mode the random plaintext and key has been taken in integer form and after process the cipher text in integer form has been converted into character. Finally we accumulate the 10 set of plaintext, cipher text and key. We generate the 10 samples (plaintext, key and its corresponding cipher text) in the form of character which has been explained in the Table 1. In the table we observe that a [■] character has frequently occurred but the ASCII value of each [■] character is different. The maximum and minimum ASCII value of [■] character is 127 and 159 respectively, which mean ASCII value of [■] character varies from 127 to 159.

	Plaintext	Key	Cipher text
1	hi abhishek it h	sandeepmahapatra	á¼Ç }÷#¯ úávã f
2	¹êõ&ö L■ÖrÝA■-┤	■Ý©e↑'SÂ'■┼■ü↕■	Ä¾■å -¾˚Sˡ »■b`
3	ó■)■fö<<-☼%Ø= LÍ|	»c<îỳ■}|+Ú®■G■à	*Ih(■¹Ú#0M³■«d&)
4	Ë■¹ö┴ïÛÅU9¶■Ö&«	'*Tæb■§_←■ ├iØ;É	á c p■Iæ%ïþëR"■ô
5	j_☼ó └æ■sz ÇÓ!!+þw	;77f↕■î■>xÃò¾Ú¹=	âQ ù┐ £=û☼┐◄C$xËW
6	/ÌJëJwzZ ^■{ã¹ô ¯-	Ùf+¿¾6Ób■Ô Ò±■ç┌rj	S³Ø ■Òk˚ âóIàÇDÁ
7	ÌÎEb ëb*,Ëüó■ú	■Õó0˙ä,Ø■6!Øze6«	3■ =(¹¿»þ{←■i¿ └
8	¥£ñ? ØB»ì»˚=♂ÑUx[	■æ}9→Ì g=ÈzããÄ■˙	■zΰì ¯!!ôü Ü Ý♫+
9	■\&┘ s¶.■{[¥è ┤U/	■x ■öÍ®tÉ4[?ý9■¸	■8-Ý RÚ¿ I■Ou■
10	r=& JÃ↕D/þ■R☼Ó;	♫■?;♂ÍÜ®v>↕§²L 9	Ì É[à■AP◘É"■³I!

Table 1: Set of Random Plaintext, Key with its corresponding Cipher text

V. Conclusions

As the final result shown in the Table 1 proofs cryptanalysis is not possible in AES (Advance Encryption Standard). The plaintext has been taken randomly which include special character also, as a result we obtain some absurd cipher text after the encryption process, which clearly shows that it is not possible to find out pattern or we cannot find out the skeleton of the plaintext with the help of cipher text structure. But one pattern that comes out from the result is that the character alphabet (A-Z) or (a-z) hasn't transformed into '[■]' character. It always been a special character which has been transformed into that particular character but as I mentioned above that there is no fix ASCII value of [■] character it's ASCII value lies in between 127 to 159 in our experiment. But still attacker never finds out the actual plaintext on the basis of this pattern because firstly there is large variety of special character and secondly the ASCII value is not fix for the [■] character. On the basis of this evaluation we must say that the AES (Advance Encryption Standard) is most secure symmetric cipher and the performance of AES is very high because of its high complexity with CBC.

REFERENCES

[1] B. Schneier, Applied Cryptography, second edition. John Wiley & Sons, Inc. New York, 1996.

[2] El-Sayed Abdoul, Waleed A. El-masry, Allaa El-Din Sayed Hafez. "A New Chaos Advance Encryption Standard (AES) Algorithm for Data Security". ICSES 2010 Gliwice, Poland, September 7-10,2010

[3] D. R. Stinson. "Cryptography, Theory and Practice", Second edition. Chapman & WalllCRC Press, 2002.

[4] Xinsheng Wang, Liang Han, Chenxu Wang, Xiaoning Liu. "Based MATLAB on Advance Encryption Standard (AES) IP Validation". IEEE- 2008

[5] Jorg J. Buchholz. "MATLAB Implementation of the Advance Encryption Standard" December 19, 2001

[6] M.Doulcier, M.L. Flottes, B. Rouzeyre. "AES based BIST: self test, test pattern generation and Signature analysis". 4th IEEE International Symposium on Electronic Design, IEEE-2008

[7] FIPS 197, "Advanced Encryption Standard," Federal Information Processing Standard (FIPS). Publication 197, Nationil Bureau of Standards, ' US. Department of Commerce, Washington D.C., November 26 2001

[8] Valeri Tomashau, Tom Kean "Validation of an Advance Encryption Standard (AES) IP Core". FCCM-2004, 12th IEEE Symposium on Field Programable Custom Computing Machines.

[9] Brain Gladman "Implementation of AES (Rijndael) in C/C++ and Assembler,"

[10] William Stallings, "Cryptography and Network Security", Pearson Education, third Edition 2008