Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 7; October, 2014 pp. 19-24

http://www.krishisanskriti.org/jbaer.html

A Survey on Ensemble of Modifications on AES Algorithm

Niharika Tyagi[1], Priyanka[2]

[1]*Uttar Pradesh Technical University, Lucknow.*
[2]*G. B. Pant Govt. Engineering College, Delhi*

Abstract: In today's era, due to rapid advancements in multimedia communication, multimedia encryption schemes have been increasingly studied applied to make the communication over an insecure channel such as global internet, for ease of transmission of confidential data in a secure, and reliable manner. To meet such challenges, available cryptographic techniques are essential to be modified. In this paper, various modifications that have been proposed on AES algorithm that have been developed to decrease its time complexity on bulky data and increased security will be included using image as input data. The modifications proposed varies itself including alteration in the S-box or shift rows transformation of AES encryption algorithm, embedding confusion-diffusion.

Keywords: Advanced Encryption Standard (AES), encryption, key, Shiftrows, S-box, state, Permutation, Affine Transformation.

1. INTRODUCTION

The Advanced Encryption Standard (AES) is given by the National Institute of Standards and Technology for the encryption of text, image or audio, video or any multimedia data. It is given by Joan Daemen &Vincent Rijmen therefore AES algorithm is also known as Rijndael which is a standard in October 2001 .AES is widely used for encrypting all forms of multimedia and digital data send over insecure networks. Encryption transforms data to some scrambled form called cipher text while decryption converts the scrambled text back to original form called plaintext.

AES uses the same key for encoding and decoding of data for which it is also known as symmetric block cipher, implements block length of 128 bits, with three key length options of 128-bits, 192-bits and 256-bits .There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for processing 256-bit keys while encryption..All the rounds are identical, last round being an exception [3]. AES algorithm uses

Galois field (GF) with 2^8 elements, also known as GF (256). There are many changes which are proposed in AES algorithm by several researchers to make AES more secure, but with reduced time complexity. The various approaches include the S-box optimization by introducing some changes in construction method, adjusting Shift Rows phase to reduce the time complexity with the aim of minimizing the statistical correlation between original data and cipher data .using Permutation to implement diffusion so as to reduce overhead on complex multimedia data [1].

2. OVERVIEW OF THE AES ALGORITHM

The round function involves one substitution step, ShiftRows for permutation, a column –wise mixing phase and the Round Key addition. These 4 transformations are invertible in nature. The 128-bit block of data to be encrypted is reshaped in a 4x4 matrix of bytes known as state matrix. A word consists of. 32 words or 4 bytes. So each column of state array is a word. Before initiating rounds for for encryption; the encryption algorithm performs a prerequisite processing step that's AddRoundkey in the specification. AddRoundkey performs a byte-by-byte XOR operation on the State matrix. The state array consists of Nr =4 and Nc columns with Nc=(4, 6, and 8) where Nr & Nc denotes number of rows and columns respectively, depending on the length of encryption key selected by user. Each processing round of AES algorithm takes input state matrix and produces output matrix which is encrypted.

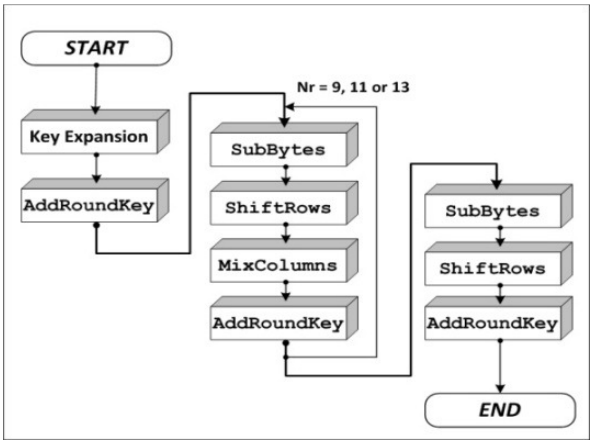

Fig. 1: Description of AES encryption algorithm[9].

The decryption algorithm is different from the encryption algorithm as the transformations used are the same but the order in which the steps are carried out is different. The AES algorithm is based on permutations and substitutions. Permutation creates diffusion in data while substitution creates confusion in data [3].Steps for Encryption, each round consists of these 4 steps-

1. **Substitute bytes:** Sub Bytes transformation is a byte substitution using a substitution table named SBox. This substitution operation takes each byte in the State matrix and puts a new byte as per the SBox table [4]. It is a 16 × 16 matrix; the entries in this matrix are created by using multiplicative inverse followed by affine transformation to destroy the bit level correlation in each byte [3].

2. **Shift rows:** This permutation step rotates bytes in the State matrix to the left. Row 0 of is rotated 0 positions to the left, row 1 is rotated 1 position left, row 2 is rotated 2 positions left, and row 3 is rotated 3 positions left [4].

3. **MixColumn:** This substitution operation is responsible for inter-byte diffusion .Each column of state matrix is multiplied with a fixed polynomial matrix [5].

4. **AddRoundkey:** The AddRoundkey operation is the same as the preliminary AddRoundkey except that each time AddRoundkey is called; the next four rows of the key schedule are used [4].

5. **The Key Expansion:** The AES encryption and decryption algorithms use a key schedule generated from the seed key array of bytes. Multiple keys from an initial keys are used so as to increase the diffusion in bits by some amount. The new keys computed from key expansion are called the round keys, this way they are distinguished from the original key [4].

3. APPROACHES APPLIED TO AES

A. Approach to generate Variable S-box using S-box rotation [5]

To construct key-dependent S-box, S-box rotation is used in key conjunction with key expansion phase.

The variable S-box will be more secure over fixed S-box as it will be dependent on key. The attacker can study the S-box easily if it remains constant throughout encryption . In recent few years several cryptanalysis attacks on block cipher urge for some changes in the algorithm. Henceforth variable S-box is proposed as it will change according to round and key used. Original AES includes 4 steps but the new AES will require 5 steps as Round function will be preceded by an additional phase known as S-box rotation. So phases will be – S-box rotation, Sub bytes, Shift Rows, MixColumns, AddRoundkey, then after final phase state becomes the output matrix.

Procedure for rotation of S-box

1. Using key schedule, round key can be derived from cipher key.
2. The derived c round key is used to calculate value which will be used to rotate S-box.
3. After having obtained round key for round say, r then apply exor operation on all bytes.
4. The result obtained after xoring will be used to rotate the S-box. This process is repeated to obtain all the 256 values of S-box. 7D558EAC0E403CD82D95275E37199242, applying exor operation on all bytes then result is 9F and 9F is used to rotate the S-box.

This algorithm is tested by the authors taking Avalanche effect into consideration .It is an important characteristic of encryption algorithm. In Avalanche effect we check for that small change in cipher key or plaintext that gives larger changes in cipher text. A secure cipher should exhibit avalanche effect to a certain degree. The simulation results on 20, 000 samples, the number of times original AES exhibit Avalanche effect is 8754 while Modified a algorithm based on S-box rotation gives better results as it shows the same for 8802 number of times [5].

B.Approach to modify AES algorithm by employing Permutation operation in place of Mix Columns [2, 6].

When we use the encryption algorithms for the security of complex multimedia data, computational overhead is so large that encryption becomes a hectic task. To overcome the computational overhead associated with large-sized data requiring hectic calculations, this new approach is analyzed to modify AES algorithm, this new modified AES algorithm improves the encryption performance, without compromising security of data. The block length is 128 bits with three key length 128, 192 & 256 bits. The 4 phases of conventional AES constituting the round function which are Sub Bytes, Shift Rows, MixColumns and AddRoundkey .But the modified AES proposed is using Permutation in place of MixColumn step. We know that, MixColumn provides better security as it plays a significant role in mixing up of the bytes serving diffusion but it requires larger calculation that makes the encryption algorithm slow. All other stages remain intact. So, modified algorithm defines stages as: Sub Bytes, Shift Rows, Permutation, and AddRoundkey.

Permutation is used in cryptographic algorithms as permutation operations are significant as they provide diffusion. Diffusion requires that each bit of plaintext block or key block should affect many bits of cipher text block and the

more the diffusion, the decryption becomes more tedious. Let x, a & k be 8-bit plaintext, cipher text and key [10].

a1=x1+x2+x3+x4+k1+K2+k3+k4
a2=x2+x3+x4+x5+K2+k3+k4+k5
a3=x3+x4+x5+x6+k3+k4+k5+k6
a4=x4+x5+x6+x7+k4+k5+k6+k7
a5=x5+x6+x7+x8+k5+k6+k7+k8
a6=x6+x7+x8+x1+k6+k7+k8+k1
a7=x7+x8+x1+x2+k7+k8+k1+K2
a 8=x8+x1+x2+x3+k8+k1+K2+k3

The permutation tables are provided by the predecessor of AES algorithm, DES algorithm. The 64-bit inputs

are given to the Initial Permutation (IP) table. In the IP table, each entry indicates a specific position of a numbered input bit constituting 64 bits in the output. The table is read from left to right and then from bottom to top therefore we can analyze that the 53 rd position tells us the 29th bit of 64 bit block The IP table is shown in Figure2.[6]

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Fig. 2: Initial Permutation Table [9]

This Modified AES algorithm takes a 128 bit block as input, Sub bytes and Shift Rows operations also work on 128-bit data, there is a need to divide the sequential bits of Shift Rows stage into 2 portions of 64 bits each and then by taking each part of 64 bits as input of permutation tables and shifts bits according to IP table taken from DES algorithm. One bit from the source is fetched and then placed into the appropriate position in target destination. Each bit is interpreted according to IP table. After having completed permutation operation on 128 bits, again we repeat it for another 128-bit set and then the remaining operations of algorithm are executed. For the decryption inverse sub bytes, inverse shift rows, inverse permutation and inverse AddRoundkey, Inverse initial permutation table is used for decryption [6].

This algorithm when used by the author to encrypt several text and image files, the modified algorithm gives better results, by providing better security with reduced overhead making it more efficient for complex multimedia data. As a 60 kb file which requires 20 seconds using original AES, can be encrypted in 8 seconds using modified AES algorithm. [6]

C. Approach to modify AES algorithm by changing the criteria for shifting in Shift Rows Transformation [2]

AES is a block cipher which is very popular as it provides confidentiality through encryption thus, preventing any unauthorized access. This modification proposed in AES algorithm promises greater security as it hides the perceptual information in an image completely .In comparison to original AES algorithm, the modified one takes less running time which makes it more applicable to real time applications, this approach for modification by bringing a change in Shift rows Transformation step of AS algorithm. The original shift rows phase is modified as:

1. If the entry in first row and first column of 4x4 state array of AES is odd then according to this modified AES algorithm, the first and third rows of state matrix are remain same while each byte of second row is shifted one to left and fourth row is shifted by three to left.

2. Else if state[0][0] is even then according to modified AES algorithm, first and fourth rows are unchanged and each byte of second row is shifted three to right and third row is shifted two to right . The algorithm given by the author is :

```
ShiftRows (byte state [4, Nb])
begin
byte t[Nb]
If state [0][0] %2! =0
for r=1:1:3
X=rmod4
If x== step 0 to x+1
for c=0:1:Nb-1
T[c] =state[r, (c+x) mod Nb]
endfor
for c=0:1:Nb-1
state [r, c]=t[c]
endfor endfor
else
for r=2:2:4
k=0
x=r mod4
If x=0:0:3
For c=Nb-1, c>=0, c-1
T[c]=state[x, (c+x)mod Nb, k+1
endfor
for c=0, c<Nb, c+1
state[x, c]=t[c] endfor endfor end
```

The simulation results when this algorithm is executed in Matlab, gives better results than the classic AES algorithm and thus the new MAES accounts for more security and increased reliable performance. In original AES, the encrypted or cipher image is such that it can be guessed or cracked by the attacker but in modified AES, the cipher image is totally invisible, leaving the attacker clueless about the image and makes the decryption of image tedious. The ultimative motive of information hiding is implemented. Experimental results when carried out on an image are as follows:

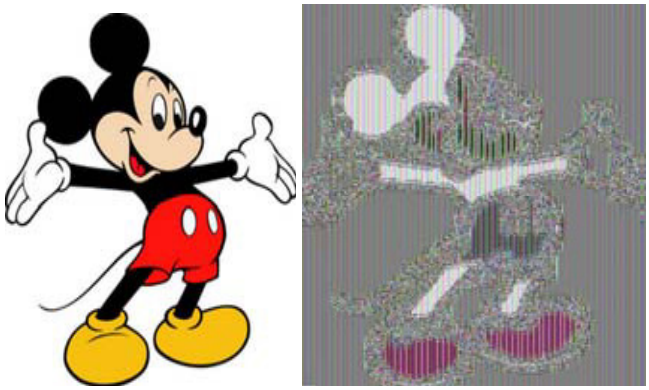

Fig. 3: AES applied to above plain image on the left and encrypted image on the right [2]

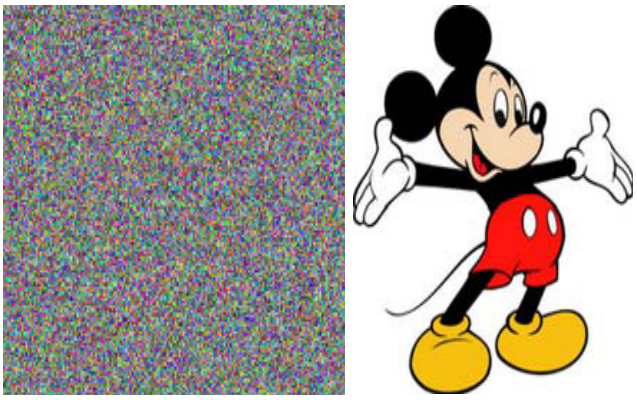

Fig. 4: MAES-128 applied to the plain image on the left and encrypted image on right [2].

With MAES algorithm, comparative performance analysis of images using AES & MAES.

Table 1. Comparison of performance of AES with MAES [2]

Size of image	Encryption time(ms), [AES]	Encryption time(ms), [MAES]
256x256	6.443	6.349
1024x1024	75.862	75.114

D. Approach to change S-box of AES by altering its construction to modify AES algorithm [1].

A new approach proposed is to modify the formulation process of S-box lookup table of size 16*16. To reduce the time complexity of AES, the affine transformation involved in the construction of S-box is modified .S-box which implements the confusion or substitution operation, is one of the most important components of as the substitution bytes step tries to reduce the correlation between the input data bits and output data bits.

The construction of S-box includes these two transformations (a) GF (2^8) arithmetic multiplicative inverse operation followed by an affine transformation. S-box is constructed by combination of both. During decoding phase, firstly an inverse affine transformation is implemented and then the multiplicative inverse is calculated [3]. In classis AES algorithm, the 2 steps are defined as Firstly, Multiplicative inverse is used to replace each byte in state array is using the polynomial $x^8+x^4+x^3+x+1$ and second is The affine transformation in the finite field GF (2^8) is given by equation:

$bi'=b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$, the constant being {63}. [1]

Due to the fact that S-box is very time consuming, new affine transformation uses the equation-
$bi'=b_i \oplus b_{(i+1)mod8} \oplus b_{(i+7) \bmod 8} \oplus c_i$, c_i is {54}
$bi'=b_i \oplus b_{(i+2)mod8} \oplus b_{(i+3) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus c_i$, c_i is 38 in decimal, i can take values from 0 to 8.[1]

But before implementing the new affine transformation, the first step is to check whether the linear equation which is to be implemented is a valid affine transformation or not. To proceed, we will analyze the equation by representing it in form of 8*8 matrixes. The first row of matrix will contain 1 corresponding to the equation and rest of the elements will be zero. The remaining 7 rows are formulated by circular shifting the previous row right by 1 bit. Now, the First row of the matrix is interpreted in the form:$a_7a_6a_5a_4\ a_3a_2a_1a_0$. Then all the 8-bit possible values are represented as $b_7b_6b_5b_4b_3b_2b_1b_0$. To check for valid affine transformation, the condition is given by-

$Ifa_7.b_0 \oplus a_6.b_1 \oplus a_5.b_2 \oplus a_4.b_3 \oplus a_3.b_4 \oplus a_2.b_5 \oplus a_1.b_6 \oplus a_0.b_7=1$ $\&\&a_7.b_7 \oplus a_6.b_0 \oplus a_5.b_1 \oplus a_4.b_2 \oplus a_3.b_3 \oplus a_2.b_4 \oplus a_1.$ $b_5 \oplus a_0.b_6=0 AND a_7.b_6 \oplus a_6.b_7 \oplus a_5.b_0 \oplus a_4.b_1 \oplus a_3.b_2 \oplus a_2.b_3 \oplus a_1.b_4$ $\oplus a_0.b_5=0$ $\&\&a_7.b_4 \oplus a_6.b_5 \oplus a_5.b_6 \oplus a_4.b_7 \oplus a_3.b_0 \oplus a_2.b_1 \oplus a_1.b_2 \oplus a_0.b_3=0\&\&$ $a_7.b_5 \oplus a_6.b_6 \oplus a_5.b_7 \oplus a_4.b_0 \oplus a_3.b_1 \oplus a_2.b_2 \oplus a_1.b_3 a_0.b_4=0\&\&a_7.b_3$ $\oplus a_6.b_4 \oplus a_5.b_5 \oplus a_4.b_6 a_3.b_7 \oplus a_2.b_0 \oplus a_1.b_1 a_0.b_2=0\&\&a_7.b_2 \oplus a_6.b_3$ $\oplus a_5.b_4 \oplus a_4.b_5 \oplus a_3.b_6 \oplus a_2.b_7 \oplus a_1.b_0 \oplus a_0.b_1=0\&\&a_7.b_1 \oplus a_6.b_2 \oplus a_5$ $.b_3 \oplus a_4.b_4 \oplus a_3.b_5 \oplus a_2.b_6 \oplus a_1.b_7 \oplus a_0.b_0=0$ then $a_7a_6a_5a_4a_3a_2a_1a_0$ will be valid affine transformation.[1] During decryption, the

equation for the inverse affine columns will be bi'= b(i+2)mod8 ⊕ b(i+5) mod 8⊕b(i+7) mod8 ⊕ b(i+7) mod8 ⊕ ci, the constant being {05} defines, where i takes values from 0 to 7, b_i is the i^{th} bit of the byte and c_i is the i^{th} bit of constant byte c [1].

E. Approach to make AES algorithm more reliable and robust by increasing key size [11].

The classic AES encryption algorithm is a secret-key cryptography that uses 128, 192, 256 bit encryption keys and it makes 10, 12 & 14 iterations depending on key length .An approach proposed is to increase the robustness of AES algorithm which can be achieved by increasing the key length to 384, 512, 768 and 1024 bits, on data matrices of 8*6, 8*8, 8*12 and 8*16 bytes which means data matrices of 48, 64, 96 & 128 b ytes respectively[11] . The maximum key length of 256 bits has been increased to maximum of four times as 1024 is 4 times of 256. Also this proposed modification offering large key space offers resistance to brute force which is an exhaustive search attack method that tries for all combinations of possible keys due to the fact that larger key dimension will make the task of analyzing the set of possible keys a tedious and perplexing one. [12]. Due to the fact AES encryption algorithm works on finite algebraic fields (Galois Field), denoted by GF(2^n), all the arithmetic operations addition, subtraction, multiplication etc .are defined on the Galois field as Galois filed is widely applied in cryptography since each data byte are manipulated as a vector or element in Galois field also known as finite field, encoding and decoding using mathematical arithmetic is easily computable . Galois field is a field with finite no of elements [13]. All the operations and computations in GF are simple and there are various fast algorithms for computations in GF .The modified algorithm uses state matrix be having 8 rows which is always fixed but number of columns vary according to encryption key length. The no of columns will be 6, 8, 12, 16 when the encryption key length is 384, 512, 768 and 1024 respectively.

The modifications in the phases of original algorithm is carried out in this manner: The first phase Sub bytes remains the same .The second step ShiftRows will be modified according to the state matrix, rows will be shifted by with magnitude 0-7 instead of 0-3. I^{st} row is not shifted, 2^{nd} row shifted one to left, 6^{th} row is shifted five to left and 8^{th} row s shifted seven to left. Then to carry out the Mix Columns transformation uses the invertible polynomial $A(x)=x^7+2x^6+3x^5+4x^4+5x^3+6x^2+7x+8$ for encryption .The matrix derived from it is as follows: A=eqn22.There is a flexibility allowing you to select a secret encoding polynomial but it should be checked for the invertible condition. Thus, this approach has increased the key size, which therefore increases the size of matrices and encryption polynomial matrices without increased overhead of time complexity.

It is concluded that the increased number of iterations and larger key length are the 2 important parameters to ensure the security and robustness of this algorithm. . The algorithm with a fewer number of iterations is more prone to various cryptanalysis attack.

4. CONCLUSION

The various modified AES algorithms proposed are more robust than the original AES as they have been tested on various parameters of security and modified algorithm has proved to give better encryption results with reduced time complexity. A good encryption algorithm should resist various kinds of attacks say, known plain-text attack, and several other brute –force attacks.

Using the Modified AES algorithm based on adjusting ShiftRows phase yields better results as coefficient for plain image is 0.9452 while for cipher image is 0.0112, there is a great difference between the two[2]. Moreover, Histograms of encrypted &original image are analyzed. The histogram of an image depict the image statistics, a good encryption algorithm should encrypt cipher image in such a way that it bears no or minimum statistical similarity to the histogram of plain image. So the histograms of plain and cipher image should be far different so attacker can find no correlation to decrypt it[2]. Another important parameter is Key space, AES uses a symmetric key of 256 bits, resulting in a key space containing 2^{256} possible keys[8] .AES uses confusion and diffusion that aid in preventing statistical analysis and it is enhanced with the techniques included in the paper

The various modified AES algorithms proposed are more robust than the original AES as they have been tested on various parameters of security and modified algorithm has proved to give better encryption results with reduced time complexity. A good encryption algorithm should resist various kinds of attacks say, known plain-text attack, and several other brute –force attacks. Using the Modified AES algorithm based on adjusting ShiftRows phase yields better results as coefficient for plain

REFERENCES

[1] Oyshee Brotee Sahoo, Dipak K Kole, Hafizur Rahaman, An Optimized S-Box for Advanced Encryption Standard(AES) Design, International Conference on Advances in Computing and Communications, ©2012 IEEE

[2] Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, Abd El Fatah. A. Hegazy, "An Efficient MAES Adapted for Image Cryptosystems ", International Journal of Computer science & "Network Security .Vol. 10 No. 2, February 2010.

[3] "Salient Features of AES". Available at https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf. Accessed on 19-05-14

[4] “Overview of AES algorithm “. Available at http://msdn.microsoft.com/en-us/ magazine/cc164055.aspx. Accessed on 10-08-2014

[5] Julia Juremi, Ramlal Mahmod, Salasiah Suleman, JazrinRamli, “Enhancing Advanced Encryption Standard S-Box Generation Based On Round Key”, (IJCSDF)1(3):183-188(SDIWC)2012(ISSN:2305-0012).

[6] “Vandana Koradia, "Modification in Advanced Encryption Standard ", Journal of Information, Knowledge andResearch in Computer Engineering, ISSN: 0975-6760 Nov12 to Oct 13, Volume-02, Issue-02 Page 358.

[7] http://amd-dev.wpengine.netdna-dn.com/wordpress/media/2013/01/AES_Fig_1.jpg, Figure 1: AES Forward Cipher Flow Graph

[8] “KeySpace".Availableat http://en.wikipedia.org/wiki/Key_space_ (cryptography) Accessed on 11-08-14.

[9] “Diffusion equations “.Available at http://www.cs.ust.hk/faculty/cding/COMP581/SLIDES/confdiffu.pdf, Accessed on 18-08-14

[10] Lecture Note 8, Attacks on Cryptosystems I by Sourav Mukhopadhyay, Available at http://www.facweb.iitkgp.ernet.in/~sourav/lecture_note8.pdf Accessed on 04-03-14.

[11] Lecture note 3, Mathematical Background by Sourav Mukhopadhyay, Available at http://www.facweb.iitkgp.ernet.in/~sourav/lecture_note3.pdf.Accessedon 04-08-2014