Study of Effect of Removal of Shiftrows and Mixcolumns Stages of AES and AES-KDS on their Encryption Quality and Hence Security

1Krishnamurthy G N, 2V Ramaswamy

Abstract—This paper demonstrates the results when either Shiftrows stage or Mixcolumns stage and when both the stages are omitted in the well known block cipher Advanced Encryption Standard (AES) and its modified version AES with Key Dependent S-box (AES-KDS), using avalanche criterion and other tests namely encryption quality, correlation coefficient, histogram analysis and key sensitivity tests.

Keywords—Encryption, Decryption, Avalanche, key sensitivity.

I. INTRODUCTION

In October 2000, after a four year effort to replace the ageing Data Encryption Standard (DES), National Institute for Standards and Technology announced the selection of Rijndael [1] as the proposed AES [1-3]. Here we will assume that readers are familiar with AES design. Details of modified version of AES namely AES-KDS are available in our paper [4]. In that paper we have suggested four different cases implementations of AES-KDS [4]. The encryption procedure of AES uses four stages namely Addroundkey, SubBytes, Shiftrows and Mixcolumns. AES-KDS has an extra stage Rotate_S-box. First we will study to see what happens to the performance of AES and AES-KDS if Shiftrows stage is omitted.

II. EFFECT OF REMOVAL OF SHIFTROWS STAGE

We have taken 30000 pairs of plaintexts with each pair differing in only one bit. We have encrypted them using AES algorithm (without Shiftrows stage) and have compared these values with that of the encrypted samples of AES. We have counted the number times AES gives better avalanche [2], [3] number of times AES without Shiftrows stage gives better avalanche and number of times both give the same avalanche. Tabulation of results for rounds 2, 4, 6, 8 and 10 of AES and AES without Shiftrows stage algorithms for one bit change in plaintexts is shown in table I and that for AES and Case 3 of AES-KDS without Shiftrows stage using same plaintext samples is shown in table II.

The results show that AES algorithm gives better avalanche compared to AES without Shiftrows and Case 3 of AES-KDS without Shiftrows stage. We can also observe the little contribution by the stage Rotate_S-box of AES-KDS by observing the results for 2 rounds in table I and table II. Similar Avalanche results can be observed when Mixcolumns stage is removed and also when both Shiftrows and Mixcolumns stages are removed both for AES and for AES-KDS.

III. ENCRYPTION QUALITY ANALYSIS

The quality of image encryption [6]-[10] may be determined as follows:

Let $F$ and $F'$ denote the original image (plainimage) and the encrypted image (ciphertext) respectively each of size $M \times N$ pixels with L grey levels. $F(x, y), F'(x, y) \in \{0, \ldots, L-1\}$ are the grey levels of the images $F$ and $F'$ at position $(x, y)$ $(0 \leq x \leq M-1, 0 \leq y \leq N-1)$. Let $H_2(F)$ denote the number of occurrences of each grey level L in the original image (plainimage) $F$. Similarly, $H_2(F')$ denotes the number of occurrences of each grey level L in the encrypted image (ciphertext) $F'$. The encryption quality represents the average number of changes to each grey level L and is expressed mathematically as

$$\text{Encryption Quality} = \frac{1}{256} \sum_{L=0}^{L-1} | H_2(F') - H_2(F) |$$
For all tests we have used two images Ships.bmp and Birds.bmp both of size 512x512.

We now compare the quality of encryption of AES with that of AES without Shiftrows stage and with that of Case 3 of AES-KDS without Shiftrows stage using two images Ships.bmp and Birds.bmp and their corresponding encrypted images. The results are tabulated in tables III and IV.

### TABLE III  ENCRYPTION QUALITIES USING SHIP.BMP AS PLAINIMAGE

<table>
<thead>
<tr>
<th>Number of Rounds</th>
<th>Algorithm type</th>
<th>EQ for AES without Shiftrows stage</th>
<th>EQ for AES-KDS without Shiftrows stage (Case 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>866.757812</td>
<td>1015.625000</td>
<td>1015.625000</td>
</tr>
<tr>
<td>4</td>
<td>866.781250</td>
<td>1015.625000</td>
<td>1015.625000</td>
</tr>
<tr>
<td>6</td>
<td>863.656250</td>
<td>1015.625000</td>
<td>1015.625000</td>
</tr>
<tr>
<td>8</td>
<td>867.625000</td>
<td>1015.625000</td>
<td>1015.625000</td>
</tr>
<tr>
<td>10</td>
<td>862.859375</td>
<td>1015.625000</td>
<td>1015.625000</td>
</tr>
</tbody>
</table>

### TABLE IV  ENCRYPTION QUALITIES USING BIRDS.BMP AS PLAINIMAGE

<table>
<thead>
<tr>
<th>Number of Rounds</th>
<th>Algorithm type</th>
<th>EQ for AES without Shiftrows stage</th>
<th>EQ for AES-KDS without Shiftrows stage (Case 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1400.585938</td>
<td>1413.687500</td>
<td>1470.945312</td>
</tr>
<tr>
<td>4</td>
<td>1386.945312</td>
<td>1437.015625</td>
<td>1445.835938</td>
</tr>
<tr>
<td>6</td>
<td>1402.367188</td>
<td>1441.304688</td>
<td>1445.968750</td>
</tr>
<tr>
<td>8</td>
<td>1384.312500</td>
<td>1389.234375</td>
<td>1415.437500</td>
</tr>
<tr>
<td>10</td>
<td>1396.031250</td>
<td>1426.445312</td>
<td>1415.109375</td>
</tr>
</tbody>
</table>

Even though the magnitudes of encryption quality for AES without Shiftrows stage are more than that of AES, their values differ very little for different rounds. This is a sign of poor encryption quality.

The above results show that modification done to the function does not degrade the quality of encryption.

### IV. KEY SENSITIVITY TEST

We have conducted key sensitivity test on the image Birds.bmp for AES and AES without Shiftrows and AES-KDS without Shiftrows using the 128 bit keys K1 and K2 as follows:

K1 = ADF278565E262AD1F5DEC94A0BF25B27 (Hex)
K2 = ADF278565E262AD1F1DEC94A0BF25B27 (Hex)

For AES algorithm, the results are already shown in figure 1(figures 1A through F). The encrypted image (encrypted with K1) differs from the encrypted image (encrypted with K2) in 99.453354% of pixels.

This experiment is repeated for AES without Shiftrows, AES without Mixcolumns and without both. The encrypted image (encrypted with K1) differs from the encrypted image (encrypted with K2) by 24.836978%, 68.482422%, 24.773895% of pixels for AES without Shiftrows stage, AES without Mixcolumns stage, and AES with both the stages removed respectively. These results show that Shiftrows stage is more sensitive to key change than Mixcolumns stage.

Encrypted images of Birds.bmp for AES without Shiftrows stage using keys K1 and K2 are shown in figures 2B and 2C, for that of AES without Mixcolumns stage are shown in figures 3B and 3C, and for AES with both the stages removed are shown in figures 4B and 4C. From the figures we can observe the appearance of traces of original image which is an indication of poor encryption. This makes cryptanalysis very easy leading to the retrieval of original information without much difficulty. For removal of Shiftrows or Mixcolumns or both stages, when we tried to decrypt images encrypted with K1 and K2 using keys K2 and K1 respectively, decryption reveals much information about the original image. The results are shown in 2E and 2F for AES without Shiftrows stage, 3E and 3F for AES without Mixcolumns stage and for AES with both the stages removed the results are shown in 4E and 4F. The amount of information revealed for AES without Shiftrows stage is much more when compared to what is revealed for AES without Mixcolumns stage. So the contribution of Shiftrows stage is more to key sensitivity than Mixcolumns stage.

This experiment is repeated (Case 3 of modified AES-KDS). Percentages of number of pixels that differ from the image encrypted with K1 with that image encrypted with K2 for AES-KDS without Shiftrows stage, AES-KDS without Mixcolumns stage, and AES-KDS with both the stages removed are 99.657234%, 99.929985%, 99.950760% respectively. Here percentage difference is huge compared to that of AES. This difference is computed based on the corresponding pixels in the encrypted images encrypted using keys K1 and K2. The additional stage Rotate_S-box has its own influence in mixing pixels. The textures visible in the encrypted images using AES reveal more information than that are visible in Case 3 of AES-KDS. These results show that Shiftrows stage is more sensitive to key change than Mixcolumns stage.

Encrypted images of Birds.bmp using AES-KDS without Shiftrows stage with keys K1 and K2 are respectively shown in figures 5B and 5C, for that of AES-KDS without Mixcolumns stage are shown in 6B and 6C, and for AES-KDS with both the stages removed they are shown in 7B and 7C. For these three types, when we tried to decrypt images encrypted with K1 and K2 using keys K2 and K1 respectively, decryption reveals much information about the original image. The results are shown in 5E and 5F for AES-KDS without Shiftrows stage, 6E and 6F for AES-KDS without Mixcolumns stage and for AES with both the stages removed they are shown in 7E and 7F. The amount of information revealed for AES-KDS without Shiftrows stage is much more than what is revealed for AES without Mixcolumns stage. So the contribution of Shiftrows stage is more to the key sensitivity than Mixcolumns stage.
Fig. 1 Results of Key Sensitivity analysis for Original AES Algorithm

Fig. 1A Plain image Birds.bmp

Fig. 1B Encrypted with Key K1

Fig. 1C Encrypted with Key K2

Fig. 1D Difference of Images in 1B & 1C

Fig. 1E Encrypted with Key K1 but Decrypted with K2

Fig. 1F Encrypted with Key K2 but Decrypted with K1

Fig. 1 Results of Key Sensitivity analysis for Original AES Algorithm
Fig. 2 Results of Key Sensitivity analysis for AES Algorithm without Shifttrows stage

- Fig. 2A Plainimage Birds.bmp
- Fig. 2B Encrypted with Key K1
- Fig. 2C Encrypted with Key K2
- Fig. 2D Difference of Images in 2B & 2C
- Fig. 2E Encrypted with Key K1 but Decrypted with K2
- Fig. 2F Encrypted with Key K2 but Decrypted with K1

Fig. 2 Results of Key Sensitivity analysis for AES Algorithm without Shifttrows stage
Fig. 3A Plainimage Birds.bmp

Fig. 3B Encrypted with Key K1

Fig. 3C Encrypted with Key K2

Fig. 3D Difference of Images in 3B & 3C

Fig. 3E Encrypted with Key K1 but Decrypted with K2

Fig. 3F Encrypted with Key K2 but Decrypted with K1

Fig. 3 Results of Key Sensitivity analysis for AES Algorithm without Mixcolumns stage
Fig. 4A Plainimage Birds.bmp

Fig. 4B Encrypted with Key K1

Fig. 4C Encrypted with Key K2

Fig. 4D Difference of Images in 4B & 4C

Fig. 4E Encrypted with Key K1 but Decrypted with K2

Fig. 4F Encrypted with Key K2 but Decrypted with

Fig. 4 Results of Key Sensitivity analysis for AES Algorithm without Shiftrows and Mixcolumns stages
Fig. 5 Results of Key Sensitivity analysis for Case 3 of AES-KDS Algorithm Without Shiftrows stage
Fig. 6 Results of Key Sensitivity analysis for Case 3 of AES-KDS Algorithm without Mixcolumns stage

Fig. 6A Plainimage Birds.bmp
Fig. 6B Encrypted with Key K1
Fig. 6C Encrypted with Key K2
Fig. 6D Difference of Images in 6B & 6C
Fig. 6E Encrypted with Key K1 but Decrypted with K2
Fig. 6F Encrypted with Key K2 but Decrypted with K1
Fig. 7A Plainimage Birds.bmp

Fig. 7B Encrypted with Key K1

Fig. 7C Encrypted with Key K2

Fig. 7D Difference of Images in 7B & 7C

Fig. 7E Encrypted with Key K1 but Decrypted with K2

Fig. 7F Encrypted with Key K2 but Decrypted with K1

Fig. 7 Results of Key Sensitivity analysis for Case 3 of AES-KDS Algorithm without Shiftrows and Mixcolumns stages
V. STATISTICAL ANALYSIS

This is shown by a test on the histograms [6]-[10] of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

A. Histograms of Encrypted Images

We have selected Ship.bmp image as plainimage for histogram analysis. We have encrypted this image first by using AES without Shiftrows stage, then by using AES without Mixcolumns stage and finally by using AES with both the stages omitted. Then we have generated histograms for plainimage and its encrypted images.

Figure 8 shows the histogram for original image. Figures from 9 to 11 show histograms for encrypted images we just obtained. From figure 9B we can see that the histogram of the encrypted image (figure 9A) encrypted using AES without Shiftrows is fairly uniform and is significantly different from that of the original image. But the other two histograms (figures 10B and 11B) for encrypted images encrypted using AES without Mixcolumns and AES with both stages omitted, they are not uniform.

The percentages of number of pixels with a certain grey scale value range from 0 to 1% and 0 to 1.8% respectively for the last two cases where as it is around 0.4% for the first case. This shows the importance of Mixcolumns stage.

Similarly, we have encrypted plainimage (Ship.bmp) first by using AES-KDS (Case 3) without Shiftrows stage, then by using AES-KDS (Case 3) without Mixcolumns stage and finally by using AES-KDS (Case 3) with both the stages omitted. Then we have generated histograms for plainimage and its encrypted images.

Figures from 12 to 14 show histograms for encrypted images we just obtained. From figure 12B we can see that the histogram of the encrypted image (figure 12A) encrypted using case 3 of AES-KDS without Shiftrows is fairly uniform and is significantly different from that of the original image. But the other two histograms (figures 13B and 14B) for encrypted images encrypted using case 3 of AES-KDS without Mixcolumns and case 3 of AES-KDS with both stages omitted, they are not uniform.

The percentages of number of pixels with a certain grey scale value range from 0 to 1.1% and 0 to 1.8% respectively for the last two cases where as it is around 0.4% for the first case. This shows the importance of Mixcolumns stage.

The percentages of number of pixels with a certain grey scale value range from 0 to 1.1% and 0 to 1.8% respectively for the last two cases where as it is around 0.4% for the first case. This shows the importance of Mixcolumns stage.
Fig. 10A Encrypted Image of Ship.bmp

Fig. 10B Histogram of Encrypted Image

Fig. 10 Encrypted Image of Ship.bmp using of AES without Mixcolumns and its Hitogram

Fig. 11A Encrypted Image of Ship.bmp

Fig. 11B Histogram of Encrypted Image

Fig. 11 Encrypted Image of Ship.bmp using of AES with both Shiftrows and Mixcolumns stages omitted and its Hitogram

Fig. 12A Encrypted Image of Ship.bmp

Fig. 12B Histogram of Encrypted Image

Fig. 12 Encrypted Image of Ship.bmp using Case 3 of AES-KDS without Shiftrows and its Hitogram
To determine the correlation between horizontally adjacent pixels [6] - [10] in an image, the procedure is as follows:

First, randomly select N pairs of horizontally adjacent pixels from an image. Compute their correlation coefficient using the following formulae

\[
E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i,
\]

\[
D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2,
\]

\[
\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),
\]

\[
r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}}.
\]

where \( x \) and \( y \) represent grey-scale values of horizontally adjacent pixels in the image. \( E(x) \) represents the mean of \( x \) values, \( D(x) \) represents the variance of \( x \) values, \( \text{cov}(x, y) \) represents covariance of \( x \) and \( y \) and \( r_{xy} \) represents correlation coefficient.

We have randomly selected 1200 pairs of two adjacent pixels from the plainimage Ship.bmp and its corresponding cipherimages encrypted first by using AES without Shiftrows stage, then by using AES without Mixcolumns stage and finally by using AES with both the stages omitted. Then we have generated histograms for plainimage and its encrypted images.

Then we have computed the correlation coefficient using the above equations.

The correlation coefficient for plainimage was found to be 0.962353. For cipherimage encrypted using AES without Shiftrows stage it is 0.009232, for cipherimage encrypted using AES without Mixcolumns stage it is 0.042035 and for cipherimage which is encrypted using AES with both the stages omitted, it is 0.057859. Figures 15 through 18 show the correlation distribution of two horizontally adjacent pixels for plainimage Ship.bmp and the encrypted images encrypted using AES without Shiftrows, AES without Mixcolumns and AES with both the stages omitted, respectively.

Similar results can be observed for AES-KDS with omitted stages. For cipherimage encrypted using case 3 of AES-KDS without Shiftrows stage it is 0.009232, for cipherimage encrypted using AES-KDS without Mixcolumns stage it is 0.042035 and for cipherimage which is encrypted using Case 3 of AES-KDS with both the stages omitted, it is 0.057859. Figures 19 through 21 show the correlation distribution of two horizontally adjacent pixels for plainimage Ship.bmp and the encrypted images encrypted using AES-KDS without Shiftrows, AES-KDS without Mixcolumns and AES_KDS with both the stages omitted, respectively.

The correlation distribution graphs show similar results for all cases and hence we cannot draw a clear cut inference from these. But correlation coefficients for AES-KDS without these stages appear to have lesser magnitudes compared to that of AES with omitted stages.
VI. CONCLUSION

We have made an attempt to analyze the security of original and modified version of AES algorithm after removal of either shiftrows or mixcolumns or both the stages. By this, we have shown the importance of these two stages and their contribution to the security of the algorithms.

REFERENCES

Krishnamurthy G N born on 15th March 1974, at Davangere, India. He has applied for membership of IAENG. He obtained his B.E. degree in Electronics & Communication Engineering from Kuvempu University in 1996 and M.Tech. degree in Computer Science & Engineering from Visveswaraya technological University, India in 2000. He has obtained his Ph.D. from Visveswaraya Technological University, India under the guidance of Dr. V Ramaswamy. He has published papers in national and international conferences, journals in the area of Cryptography. After working as a lecturer (from 1997) he has been promoted to Assistant Professor in the Department of Information Science & Engineering, Bapuji Institute of Engineering & Technology, Davangere, affiliated to Visveswaraya Technological University, Belgaum, India. He has worked as Professor and Head at Cambridge Institute of Technology and BNM Institute of Technology, Bangalore, from where he has been deputed to VTU, Belgaum and is presently working as Registrar(evaluation), Visvesvaraya Technological University, Belgaum. His area of interest includes Design and analysis of Block ciphers. Currently he is guiding two Ph.D. scholars under Visvesvaraya Technological University, Belgaum. He is a life member of Indian Society for Technical Education, India.

Dr. V Ramaswamy obtained his Ph.D. degree from Madras University, in 1982. He has applied for the membership of IAENG. He is working as Professor and Head in the Department of Information Science and Engineering. He has more the 25 years of teaching experience including his four years of service in Malaysia. He is guiding many research scholars and has published many papers in national and international conference and in many international journals and authored one book. He has visited many universities in USA and Malaysia. He is working as research head in the department of Computer Science & Engg., at Mahaveer Jain College of Engg., Bangalore, India. He is a life member of Indian Society for Technical Education, India.