Chapter 4

Modified AES Algorithm

4.1 Introduction

The Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers: AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with their predecessor, the Data Encryption Standard (DES). The AES has now replaced DES as the preferred encryption standard.

AES is a cryptographically secure encryption algorithm. A brute force attack requires $2^{128}$ trials for the 128-bit key size. In addition, the structure of the algorithm and the round functions used in it ensure high immunity to linear and differential cryptanalysis. Attacks against AES haven’t been successful till now and it is the
current encryption standard. The AES design can be used in any application that requires protection of data during transmission through the communication network, including applications such as electronic commerce transactions, ATM machines, and wireless communication.

The AES is a universal encryption standard. It can be used for encryption of any type of data, text and other media alike. The AES finds special applications in encryption of images and other media like audio and video. Image encryption using the AES is done generally in Cipher Block Chaining mode to prevent clusters appearing in the image due to similar cipher text. Media file encryption also generally follows on similar lines.

4.2 The Advanced Encryption Standard Algorithm

The AES algorithm with the 128-bit key is explained here and the overall structure is depicted in Fig.4.1. There are 4 different stages, one is permutation and other three are substitution:

- Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
- ShiftRows: A simple permutation
- MixColumns: A substitution that makes use of arithmetic
over $GF(2^8)$

- **AddRoundKey**: A simple bitwise XOR of the current block with a portion of the expanded key

In AES, a state is a $4 \times 4$ matrix and block is a 16-byte length array. The block to state conversion is done column by column. The state to block conversion is also done column by column. The key that is provided as input is expanded into an array of forty-four 32-bit words, $w[i]$. Four distinct words (128 bits) serve as a round key for each round, these are indicated in Fig. 4.1.

![Figure 4.1: AES Encryption and decryption](image)

The decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm. This is a consequence of the particular
structure of the AES.

4.2.1 Substitute Bytes

In the SubBytes step, each byte in the array is updated using an 8-bit substitution box, the AES S-box as shown in Figure 4.2. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over \( GF(2^8) \), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points, and also any opposite fixed points.

![Figure 4.2: The SubByte Transformation](image)

4.2.2 Shift Rows

The ShiftRows step operates on the rows of the state, it cyclically shifts the bytes in each row by a certain offset as shown in Figure 4.3.
The first row is left unchanged. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed. The inverse shift row transformation, called InvShiftRows, used in the decryption, performs the circular shifts in the opposite direction for each of the last three rows, with a one-byte circular right shift for the second row, and so on.

4.2.3 Mix Column

The forward mix column transformation, called MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The transformation can be defined by the following
matrix multiplication on state shown in Eqn.(5.1)

\[
\begin{pmatrix}
02 & 03 & 01 & 01 \\
01 & 02 & 03 & 01 \\
01 & 01 & 02 & 03 \\
03 & 01 & 01 & 02 \\
\end{pmatrix}
\begin{pmatrix}
s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\
s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\
s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\
s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \\
\end{pmatrix}
= 
\begin{pmatrix}
s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\
s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\
s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\
s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \\
\end{pmatrix}
\tag{4.1}
\]

The inverse mix column transformation, called InvMixColumns, is defined by the following matrix multiplication shown in Eqn.(5.2).

\[
\begin{pmatrix}
0E & 0B & 0D & 09 \\
09 & 0E & 0B & 0D \\
0D & 09 & 0E & 0B \\
0B & 0D & 09 & 0E \\
\end{pmatrix}
\begin{pmatrix}
s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\
s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\
s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\
s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \\
\end{pmatrix}
= 
\begin{pmatrix}
s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\
s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\
s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\
s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \\
\end{pmatrix}
\tag{4.2}
\]

\section*{4.2.4 Add Round Key}

In the AddRoundKey step, the sub-key is combined with the state. For each round, a sub-key is derived from the main key using AES key schedule, each sub-key is the same size as the state. The sub-key is added by combining each byte of the state with the corresponding byte of the sub-key using bitwise Exclusive OR (XOR).

The inverse add round key transformation is identical to the forward add round key transformation, because the XOR operation is its own inverse.
4.2.5 AES Key Expansion

The AES key expansion algorithm takes as input a 4-word (16-byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a 4-word round key for the initial AddRound-Key stage and each of the 10 rounds of the cipher. The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time.

The function g consists of the following sub-functions:

- Rotate word (RotWord) performs a one-byte circular left shift on a word. This means that an input word \([b_0, b_1, b_2, b_3]\) is transformed into \([b_1, b_2, b_3, b_0]\).

- Substitute word (SubWord) performs a byte substitution on each byte of its input word, using the S-box.

- The result of steps 1 and 2 is XORed with a round constant, \(Rcon[j]\) shown in Table 4.1

<table>
<thead>
<tr>
<th>(j)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Rcon(j))</td>
<td>01h</td>
<td>02h</td>
<td>04h</td>
<td>08h</td>
<td>10h</td>
<td>20h</td>
<td>40h</td>
<td>80h</td>
<td>10h</td>
<td>36h</td>
</tr>
</tbody>
</table>
4.3 AES Decryption

The AES decryption cipher is not identical to the encryption cipher (Fig. 4.1). That is, the sequence of transformations for decryption differs from that for encryption, although the form of the key schedules for encryption and decryption is the same. This has the disadvantage that two separate software or firmware modules are needed for applications that require both encryption and decryption.

4.4 New AES algorithm

The AES algorithm consists of a static S-box and a constant mix column matrix. The possible combinations of secret key to be tried to break the algorithm are $2^{128}$ for AES-128 algorithm. Although algebraic attacks like linear and differential cryptanalysis are difficult (they need large amount of plain text and cipher), it has been shown that theoretically it may be possible to break the AES algorithm by XSL attack, by constructing multivariate quadratic equations. Since the S-box is static it is possible to construct these equations. There are nearly $256! \approx 2^{1638}$ S-boxes, if we generate any one of them, which is a key dependent S-box, it becomes very difficult to attack the AES algorithm. The mix column matrix is a static $4 \times 4$ matrix with 16-byte entries, and if we construct a
key dependent mix column matrix then cryptanalysis still becomes more difficult. The necessary condition to be satisfied for this mix column matrix is that it must be a non-singular. These two blocks are explained in the next section. All the remaining operations are the same as in the present AES algorithm.

4.4.1 Modified AES Algorithm

The procedure to generate the dynamic S-box is explained in detail in Chapter3. Choose an arbitrary key of size 16 bytes, which must be known at the receiver end also to decrypt the message. Construct a $4 \times 4$ matrix with these 16 bytes. Test for the singularity of the matrix with respect to an irreducible polynomial which is also key dependent as in dynamic S-box construction. If the matrix is singular then XOR each byte of the key with $[01_h]$, then test for the singularity. Continue the same procedure till we get a non-singular matrix. Then use this matrix to perform the mix column operation as in the original AES encryption algorithm. Fig. 4.4 and Fig. 4.5 show the block diagrams of the new encryption and decryption algorithms to encrypt or to decrypt the text, image or audio files.
Figure 4.4: Block diagram of New AES Encryption

Figure 4.5: Block diagram of New AES Decryption
4.4.2 Results

The AES algorithm was implemented in C and optimized for small program size. The program has been designed to create an executable file which can be then used for encryption and decryption purposes. The program can encrypt any type of file given by the user. The encrypted file retains the format of the original plaintext file subject to the encryption of the header. Files having a fixed header length facilitate encryption in the same format and the resulting encrypted file can be viewed with any image viewer if it is an image file; and if it is an audio file, it can be played in any media player software. The program can encrypt bitmap images bearing the ”.bmp” extension preserving its format and also preserves the format in case of media file having ”.wav” extension. Any attempt to encrypt a text file results in a text file, though the characters might not be completely visible because of ASCII-conversion that takes place while writing to a ”.txt” file. Other file formats are encrypted without preserving the format. However, for simplicity, the extension of the encrypted file remains the same as the original file. Such files can’t be played in a media player or viewed in image viewer. An attempt to open such files results in error messages due to encrypted headers. Such files can be viewed or played only after decryption which results in a file identical to the original file.
Text Files

Number of text files with different file lengths were tested, using the original AES algorithm, New AES algorithm without change in mix column matrix and with key dependent mix column matrix were tested. One example of these results are shown in Fig 4.6 to Fig 4.9. All the encrypted text files were decrypted by decryption algorithm and respective secret keys. It is found that in all cases the original files were extracted. It is also found that any one bit of any keys (secret key/auxiliary key/permute key) will lead to unreadable message.

In today's information age, communication plays an important role which contributed heavily to the growth of technology. Electronic security is increasingly involved in making communication more prevalent. Therefore, a mechanism is needed to assure the security and privacy of information that is sent over the electronic communication media. Whether the communication media is wired or wireless, both cannot be protected from unauthorized reception or interception of transmission. The method of transforming the original information into an unreadable format is called ENCRYPTION and the reverse process is called DECRYPTION of information. The study of encryption and decryption is known as Cryptography. Cryptography or communication by using secret codes was used by the Egyptians some 4000 years ago. However, the science of cryptography was initiated by Arabis since 609 A.D. Cryptography became vital in the twentieth century when it played a crucial role in the World War I and World War II. Cryptography involves the study and applications of the principles and techniques by which information is rendered unintelligible to all but the intended receiver, on the other hand Cryptanalysis is the science and art of solving cryptosystems to recover unintelligible information. Network security mainly consists of three parts namely data confidentiality, the data integrity and data authenticity. Data confidentiality is the protection of data from unauthorized disclosure. The data integrity is the assurance that data received are exactly as sent by an authorized entity. The authentication is the assurance that the communication entity is the one it claims to be. Present day Cryptography is involving three distinct mechanisms symmetric key encryption, asymmetric key encryption and hashing. In symmetric encryption or secret key cryptography, an entity A can send a message to another entity B, over an insecure channel with the assumption that an

Figure 4.6: Plain text or message
In today's information age, communication plays an important role which contributed heavily to the growth of technology, Electronic security is increasingly involved in making communication more prevalent. Therefore, a mechanism is needed to assure the security and privacy of information that is sent over the electronic communication media. Whether the communication media is wired or wireless, both cannot be protected from unauthorized reception or interception of transmission. The method of transforming the original information into an unreadable format is called ENCRYPTION and the reverse process is called DECRYPTION of information. The study of encryption and decryption is known as Cryptography. Cryptography or communication by using secret codes was used by the Egyptians some 4000 years ago. However, the science of cryptography was initiated by Arabs since 580 A.D. Cryptography became vital in the twentieth century when it played a crucial role in the World War I and World War II. Cryptography involves the study and applications of the principles and techniques by which information is rendered unintelligible to all but the intended receiver; on the other hand Cryptanalysis is the science and art of solving cryptosystems to recover unintelligible information. Network security mainly consists of three parts namely data confidentiality, the data integrity and data authenticity. Data confidentiality is the protection of data from unauthorized disclosure. The data integrity is the assurance that data received are exactly as sent by an authorized entity. The authentication is the assurance that the communication entity is the one that it claims to be. Present day Cryptography is involving three distinct mechanisms symmetric key encryption, asymmetric key encryption and hashing. In symmetric encryption or secret key cryptography, an entity A can send a message to another entity B, over an insecure channel with the assumption that an
Figure 4.9: Decrypted message with one bit change in key

Image Files

On image files Histograms and Correlation of two adjacent pixels are tested by using Mat-lab tools. The results of three image files are shown in Table 4.2 and Fig 4.10 to Fig 4.45. From the correlation plots it is found that the New AES algorithm with key dependent mix column have very low correlation coefficients.

<table>
<thead>
<tr>
<th>Original Image</th>
<th>Encrypted with</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AES</td>
</tr>
<tr>
<td>Horizontal</td>
<td>Vertical</td>
</tr>
<tr>
<td>Image 1</td>
<td>0.9258</td>
</tr>
<tr>
<td>Image 2</td>
<td>0.9831</td>
</tr>
<tr>
<td>Image 3</td>
<td>0.9621</td>
</tr>
</tbody>
</table>

Table 4.2: Correlation coefficients of two adjacent pixels
Figure 4.16: Image1 Encrypted with new AES

Figure 4.17: Image1 encrypted with modified AES

Figure 4.18: Histogram of Fig 4.16

Figure 4.19: Histogram of Fig 4.17

Figure 4.20: Correlation of Fig 4.16

Figure 4.21: Correlation of Fig 4.17
Figure 4.22: Image2

Figure 4.23: AES encrypted Image2

Figure 4.24: Histogram of Fig 4.22

Figure 4.25: Histogram of Fig 4.23

Figure 4.26: Correlation of Fig 4.22

Figure 4.27: Correlation of Fig 4.23
Figure 4.28: Image2 Encrypted with new AES

Figure 4.29: Image2 encrypted with modified AES

Figure 4.30: Histogram of Fig 4.28

Figure 4.31: Histogram of Fig 4.29

Figure 4.32: Correlation of Fig 4.28

Figure 4.33: Correlation of Fig 4.29
Figure 4.40: Image encrypted with new AES

Figure 4.41: Image encrypted with modified AES

Figure 4.42: Histogram of Fig 4.40

Figure 4.43: Histogram of Fig 4.41

Figure 4.44: Correlation of Fig 4.40

Figure 4.45: Correlation of Fig 4.41
Audio Files

The waveforms of original wave file (Fig. 4.46), encrypted wave file (Fig. 4.47) and decrypted wave file (Fig. 4.48) are shown. Each wave clipping is 5 second duration.

Figure 4.46: Waveform of the Original wave file

Figure 4.47: Waveform of the Encrypted wave file

Figure 4.48: Waveform of the Decrypted wave file
4.5 Conclusion

AES encryption and decryption algorithms are developed by using the key dependent dynamic S-box and key dependent mix column operation. Tests are conducted on the text, the image and the wave files, by changing the secret key, auxiliary key and permute key. In the case of image files it is found that the very low correlation between the adjacent pixels exists, when the encryption is done with dynamic S-box and key dependent mix column is used.