Encryption and Decryption of Text using AES Algorithm

Roshni Padate¹, Aamna Patel²

¹Assistant Professor, Computer Engineering Department, Fr. Conceicao Rodrigues College of Engineering
²Electronics Department, Fr. Conceicao Rodrigues College of Engineering

Abstract—Data Security is primary concern for every communication system. There are many ways to provide security to data that is being communicated. This paper describes a design of effective security for data communication by AES algorithm for encryption and decryption. The National Institute of Standards and Technology (NIST) has initiated a process to develop a Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard (AES), specifying an Advanced Encryption Algorithm to replace the Data Encryption Standard (DES) that expired in 1998. The Advanced Encryption Standard can be programmed in software or built with pure hardware.

Keywords—AES, Block Cipher, Cryptography, DES, NIST

I. INTRODUCTION

In the past few years security and integrity of data is the main concern. In the present scenario almost all the data is transferred over computer networks due to which it is vulnerable to various kinds of attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored.

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.

Purpose of cryptography:

1. Authentication: The process of proving one's identity. It is another part of data security that we encounter with everyday computer usage.

Just think when you log into your email, or blog account. The simple sign-in process is a form of authentication that allows you to log into applications, files, folders and even an entire computer system. Once logged in, you have various given privileges until logging out.

Some system will cancel a session if your machine has been idle for a certain amount of time, requiring that you prove authentication once again to re-enter.

The simple sign-on scheme is also implemented into strong user authentication systems. However, it requires individuals to login using multiple factors of authentication. Non-repudiation: In this, the receiver should know whether the sender is not faking.

For example, if suppose when one purchases something online, one should be sure that the person whom one pays is not faking.

2. Integrity: Many a times data needs to be updated but this can only be done by authenticated people.

3. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.

Encryption is the process of obscuring information to make it unreadable without special knowledge. Encryption has been used to protect communications for centuries, but only organizations and individuals with an extraordinary need for secrecy had made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now used in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines.

Encryption can be used to ensure secrecy, but other techniques are still needed to make communications secure, particularly to verify the integrity and authenticity of a message, for example, a message authentication code (MAC) or digital signatures. Another consideration is protection against traffic analysis. Intrusion can be taken care of by sending a signal to the receiver, the one that sends the acknowledgement signal back to the transmitter, the data will be sent only to that receiver. Thus with the use of handshaking signals intrusion can be avoided.

II. AES ALGORITHM

In January, 1997 NIST began its effort to develop the AES, a symmetric key encryption algorithm, and made a worldwide public call for the algorithm to succeed DES. Initially 15 algorithms were selected, which was then reduced down to 4 algorithms, RC6, Rijndael, Serpent and Two-fish, all of which were iterated block ciphers. The four finalists were all determined to be qualified as the AES.
The final evaluation, which also solicited worldwide public input was based on three characteristics:

i) Security: It encompassed resistance to known attacks, mathematical soundness, randomness of output and security compared to other algorithms.

ii) Cost: Encompassed encryption speed, required memory, and no licensing agreements i.e. the algorithm had to be available worldwide royalty free.

iii) Algorithm and implementation characteristics: The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm.

### Table 1

<table>
<thead>
<tr>
<th>Factors</th>
<th>DES</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Length</td>
<td>56 bits</td>
<td>128, 192, 256 bits</td>
</tr>
<tr>
<td>Block Size</td>
<td>64 bits</td>
<td>128, 192, 256 bits</td>
</tr>
<tr>
<td>Cipher Text</td>
<td>Symmetric block cipher</td>
<td>Symmetric block cipher</td>
</tr>
<tr>
<td>Developed</td>
<td>1977</td>
<td>2000</td>
</tr>
<tr>
<td>Security</td>
<td>Proven inadequate</td>
<td>Considered secure</td>
</tr>
<tr>
<td>Cryptanalysis resistance</td>
<td>Vulnerable to differential and linear cryptanalysis</td>
<td>Strong against differential and linear cryptanalysis</td>
</tr>
<tr>
<td>Possible Keys</td>
<td>$2^{56}$</td>
<td>$2^{128}$, $2^{192}$, $2^{256}$</td>
</tr>
</tbody>
</table>

AES was designed to have the following characteristics:

i) Resistance against all known attacks.

ii) Speed and code compactness on a wide range of platforms

iii) Design Simplicity

For Rijndael, the length of both the block to be encrypted and the encryption key are not fixed. They can be independently specified to 128, 192 or 256 bits. The number of rounds, however, varies according to the key length. It can be equal to 10, 12 and 14 when the key length is 128bits, 192 bits and 256 bits, respectively. The basic components of Rijndael are simple mathematical, logical, and table lookup operations. The latter is actually a composite function of an inversion over Galois Field (GF) with an affine mapping. Such structure makes Rijndael suitable for hardware implementation. Nevertheless, both hardware and software implementations have their own drawbacks. Hardware implementation is rigid as a block and key sizes must be held at fixed values. However, the running time is better compared to its software counterpart. All in all, Rijndael is considered to be the fastest algorithm in terms of the critical path between plaintext and cipher text.

### III. IMPLEMENTATION

The algorithm is based on AES Key Expansion technique.

#### A. AES Key Expansion technique in detail.

Pseudo code for AES Key Expansion: The key-expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates $4x(N_r+1)$ words. Where $N_r$ is the number of rounds.

The process is as follows
The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15). The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1, and so on.

The rest of the words (wi for i=4 to 43) are made as follows
1. If \((i \mod 4) \neq 0\), \(wi = wi-1 \oplus wi-4\).
2. If \((i \mod 4) = 0\), \(wi = t \oplus wi-4\). Here \(t\) is a temporary word result of applying SubByte transformation and rotate word on \(wi-1\) and XORing the result with a round constant.

B. Modifications in AES Key Expansion

Certain changes made in the above key expansion process improves the encryption quality, and also increases the avalanche effect. The changes are
1. The Rcon value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.
2. Both the s-box and Inverse s-box are used for the Key Expansion process which improves non-linearity in the expanded key and also improves the encryption quality.
3. We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key this improves the key sensitivity.

The above changes in the algorithm can be represented as

1) Formation of Rcon values
\[
Rcon[0]=key[12:15]; Rcon[1]=key[4:7];
Rcon[2]=key[0:3]; Rcon[3]=key[8:11];
\]

2) Using Inverse S-Box for key expansion
The ‘temp’ value used in the algorithm is formed as
\[
\text{temp} = \text{SubWord(RotWord(temp)) \ XOR InvSubWord(Rcon[i/4])};
\]
Where InvSubWord: InverseSubByte transformation table value

3) Shifting of S-box and Inverse S-box
\[
\text{Sbox_offset} = \text{sum(key[0:15])mod256};
\text{Inv_Sbox_offset} = (\text{sum(key[0:15])}*\text{mean(key[0:15])})\mod256;
\]
The initial key is represented as blocks key[0],key[1]...key[15]. Where each block is 8bits long (8*16=128 bits).

C. Steps Involved
1. Key Selection:
The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block is 8bits long (8*16=128 bits).

2. Generation of Multiple keys:
The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

3. Encryption:
Encryption is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey.

4. Decryption:
The decryption process is similar as encryption, but we use Inverse SubByte Transformation.

The whole AES structure is sketched in Figure 1.
IV. RESULTS

1. Encryption and Decryption:

   Encryption and Decryption process is carried out in MATLAB R2010a.

   In this case, we are taking plain text input as “aamna” and key as “patel”.

   The encryption and decryption results for the above key and plain text are as follows.

   Input Text: aamna
   Key: patel
   Encrypted Text: "ÄéÕÀÏcu
   Decrypted Text: aamna

V. CONCLUSION

   The proposed algorithm offers high encryption quality. There is currently no evidence that AES has any weaknesses making any attack other than exhaustive search, i.e. brute force, possible. Even AES-128 offers a sufficiently large number of possible keys, making an exhaustive search impractical for many decades.

VI. FUTURE WORK

   The same algorithm can again be modified to be used for Image Encryption and Decryption. Various algorithms were developed for image encryption like Image Encryption Using SCAN Patterns and Image Encryption Using Combinational Permutation Techniques. But they were mainly developed for single application scenario and hence had its own limitation when considering a general Image security application. Also these methods were not suitable for Real Time Applications because the algorithm either had very high security but was slow in processing or it was very fast at the prize of security.

   Hence there is a need for an algorithm that in general is applicable for all Image security applications in Real Time. Thus a method that is based on AES Key Expansion which overcomes the limitations of above mentioned algorithm is preferred.

REFERENCES


