A SECURE APPROACH FOR DATA TRANSMISSION IN COMPUTER NETWORKS USING MODIFIED ADVANCED ENCRYPTION STANDARD ALGORITHM

M. Indrasena Reddy 1, A.P Siva Kumar 2

1Research Scholar, Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India.
Asst.Prof, Dept of CSE, RGM CET, Nandyal, Andhra Pradesh, India.
2Asst. Prof, Department of Computer Science and Engineering, JNTUA, Ananthapuramu, Andhra Pradesh, India.

mir555mittapalli@gmail.com, sivakumar.ap@gmail.com

Corresponding Author: M. Indrasena Reddy

Abstract

In the internet along with other network applications, the requirement for security is increasing each day due to its wide usage. There are loads of algorithms which were established for the safe transmission of data. This paper offers a fresh approach for the generation of the key using the ‘Advanced Encryption Standard’ (AES) algorithm along with the Flower Pollination Algorithm (FPA). This combination is termed as Modified AES (MAES). Initially, a plain text of 128 bits is the input to this algorithm. This text is transmuted to a cipher text. The key generation is important for the generation of the ‘S-Box’ (substitution box). The key generation on the proposed work is done utilizing the FPA. This step is done to make the keys in such a manner that the complexities of the S-Box enhance. This ameliorates the security of the proposed work for data transmission on a network. Then encryption is done. This is followed by decryption. Finally, the 128bit plain text is retrieved at the receiver's side. The MAES algorithm was compared with other traditional cryptographic algorithms. The proposed MAES algorithm yielded exceptional results.

Keywords : Modified Advanced Encryption Standard Algorithm, Flower Pollination Algorithm, Security, Encryption, Decryption, Key

I. Introduction

In the modern decennium, communication has become the utmost desired requisite for mankind. For effectual communication, an appropriate communication channel is requisite. This channel is vulnerable to disparate attacks types. Cryptographic algorithms aids in transmitting data securely from source-destination.

https://doi.org/10.26782/jmcms.spl.3/2019.09.00002
The requisite for augmented cryptographic methodologies is elevating for securing information storage and communication [XVII].

I.i. Cryptography: Cryptography [II],[IX],[X],[XVIII] embraces transmutation of ‘plain text’ (PT) to a secret code or a ‘cipher text’ (CT). This process is executed at the sender zone and is named as encryption. The reversal process is executed at the receiver end and it is termed decryption. Cryptography is a methodology that handles the protection and encryption of messages whilst they are moved from the sender to the appropriate receiver. The sender together with the receiver exploits cipher key. This key and the message are operated to generate the encrypted form of message. Cryptography is extensively utilized because of its traits like a) authentication [XIX], b) data integrity, c) access control, d) confidentiality and e) non-repudiation in communication security [XV]. The utilization of cryptography ranges as of computer security to military purpose security [I].

I.ii. AES: It is concerned as a symmetric cryptographic algorithm [III] which is utmost secure for protecting data. This AES algorithm was presented by the ‘National Institute of Standards & Technology’ as a replacement for the DES algorithm (Data Encryption Standard). This algorithm has the competency to decrypt and encrypt data with variable key lengths of 256bits, 192bits in addition to128bits [VIII]. Some major traits of the AES algorithm are delineated here. The AES is regarded as the symmetric key centered algorithm [IV],[VII],[XXII]. It is utmost faster and stronger than triple DES [XVI]. It also upholds hardware together with software implementations.

The S-Box of this AES is a square matrix [XIII],[XXI],[XXIII]. It acts as a look-up table on a network. The algebraic term for this S-box generation is simpler in AES. So this algorithm’s security is supposed. This paper generates a solution to this prevailing problem. The key generation for the proposed MAES algorithm is executed utilizing the FPA. This maximizes the complexities of S-box. As an outcome, the security aspect is augmented in the network.

The other sections embraced in the paper is ordered as, Section 2 deals with the recent related works. Section 3 delivers a detailed account of the proposed methodology. Section 4 proffers the experiential outcomes. Lastly, Section 5 concludes this proposed paper.

II. Related Works

Numerous works were developed for securely transmitting data over a network. Some modern related works are delineated in this section. Jia et al.[XI] suggested an augmented key expansion methodology to augment the securities of AES centered key expansion. In respect of the defection of the RSA function efficacy, a double-prime number was substituted with a prime number. ‘Chinese remainder theorem’ integrated with ‘Montgomery modular multiplication’ was also developed to utilize modular exponentiation. To develop a joined encryption scheme i) the digital signature, ii) message digest, iii) digital envelope, etc. were employed. This embraced convenient key management and the finest encryption outcomes.

M. Indrasena Reddy et al.
Mohammed et al.[XIV] devised a hybridized security prototype for securing the diagnostic textual data in medical images. The devised prototype was introduced by an integration of RSA together with AES algorithms. The data was encrypted and then it was concealed in a cover image utilizing the one dimension DWT (‘discrete wavelet transform’) 1 level and 2 dimension DWT of level 2. The gray-scaled and colored images were utilized as cover images to conceal disparate textual sizes. Disparate performance metrics were assessed.

Hanqi et al.[XX] introduced a dynamic 3-layer encryption structure centered on the network and DES coding. This was executed with a lower intricacy partial key update methodology. Grounded on the theoretical examination, a novel methodology was proved to have upsides to attain dynamic transition betwixt the security and efficacy. This augmented the malleability to disparate cyber states. It was also perceived that the running ratio of the novel scheme was comparatively lower than or similar to the triple DES.

Unal et al.[V] recommended a chaos-centered hybridized encryption algorithm for secure and effectual encryption for images. The ‘Zhongtang chaotic’ scheme was picked and its dynamic analysis was executed. A chaos centered RNG (‘Random Number Generator’) was introduced. The S-Box generation algorithms were also modeled. By implementing the modeled RNG together with S-Box, a hybridized algorithm was introduced centered on AES.

Sujatha et al.[XII] presented a structure for encryption and authentication utilizing the modified ECC with PSO (‘Particle Swarm Optimization’) and CS (‘Cuckoo Search’) algorithm. This structure was employed and experimented on a sampled database. The outcomes which were attained were reliable and secured. The test outcomes confirmed that the private key was picked optimally not tiny/repetitive. Furthermore, it was ascertained that the evaluations in the public key would not attain infinity.

III. Proposed Methodology

The proposed work handles the transfer of data from sender-receiver on a computer network in a secured form. It proposes a cryptographic algorithm which is named as MAES algorithm (Modified-AES) for this augmenting security in data transfer. The sender transmits the message in PT form. This is transmuted to a CT.

Random keys are created for decrypting and encrypting the text. The generation of such keys is randomized by utilizing the FPA. This algorithm possesses a crucial role in the augmentation of securities of the cryptographic algorithm. In the receiver's side, the PT is retrieved as of the CT. The detailed depiction of this proposed scheme is delineated in fig 1.
The MAES executes all its operations on bytes instead of bits. Consider a PT which is indicated as $M$. In the proposed work, $M$ have 128 bits. The AES treats those 128 bits as blocks of 16 bytes. This PT is the input for the AES algorithm. The PT indicates the information, document or the file that is modeled to be sent from sender - receiver. This message is transmitted in a secured form. For this, a symmetric key is requisite for encryption together with decryption.

**III.i. Plain Text**

The secondary input for the MAES algorithm is the symmetric key. This key is symmetric as it is utilized for the encryption together with decryption. Here, the key which is regarded as a 128 bit round key is indicated as $k_i$. For 128 bit keys, the MAES utilize 10 rounds. Each of those rounds utilizes a disparate 128 bit round key, which is evaluated as of the former AES key.

**III.ii. Generation of Keys**

Generating key in the MAES algorithm is a crucial step. This phase influences the formation of the S-boxes. The generation of a key reliant S-box strengthens the algorithm. This is because the S-box’s strength is contingent on the created symmetric key. The key $k_i$ is created utilizing a PRNG (‘Pseudo-Random Number Generator’). A PRNG utilizes mathematical computations to create a sequence of numerical values by resembling the traits of random numeric. The PRNG performance starts with the selection of an arbitrary beginning state utilizing a seed state. As an outcome, several numbers are generated.

Besides, it is deterministic and effectual, since it is produced in a minimal time span and they are re-generated by identifying the beginning point. The PRNG’s
randomness is categorized by its entropy. Entropy is a gauge of randomness. In this proposed system, the entropy of the PRNG is augmented utilizing the FPA.

Fig. 2. Pseudo code of FPA

<table>
<thead>
<tr>
<th>Pseudo code for Flower Pollination Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize the population with random solutions</td>
</tr>
<tr>
<td>Find the best solution ( b )</td>
</tr>
<tr>
<td>Define the switch probability ( p ) in ([0, 1])</td>
</tr>
<tr>
<td>while ((t &lt; \text{MaxGeneration}))</td>
</tr>
<tr>
<td>for ( i = 1:n )</td>
</tr>
<tr>
<td>if ( \text{rand} &lt; p ),</td>
</tr>
<tr>
<td>( \text{Draw a step vector} \ V ) that obeys a Levy distribution</td>
</tr>
<tr>
<td>( \text{Perform Global pollination} )</td>
</tr>
<tr>
<td>( k_i^{n+1} = k_i^n + V(b - k_i^n) )</td>
</tr>
<tr>
<td>else</td>
</tr>
<tr>
<td>( \text{Draw} \ \beta ) from a uniform distribution in ([0, 1])</td>
</tr>
<tr>
<td>( \text{Choose} \ j ) and ( k ) randomly.</td>
</tr>
<tr>
<td>( \text{Perform Local pollination} )</td>
</tr>
<tr>
<td>( k_i^{n+1} = k_i^n + \beta(k_j^n - k_i^n) )</td>
</tr>
<tr>
<td>end if</td>
</tr>
<tr>
<td>Evaluate new solutions</td>
</tr>
<tr>
<td>If the new solutions are better, update them in the population</td>
</tr>
<tr>
<td>end for</td>
</tr>
<tr>
<td>Find the current best solution ( b )</td>
</tr>
<tr>
<td>end while</td>
</tr>
</tbody>
</table>

The FPA comprises 2 notable steps in its execution like i) global pollination and ii) local pollination. In the former step, the pollens in the flowers are taken by the pollinators like insects. Those pollens travel longer distance since the insects move and fly in an utmost longer range. This assures the pollination. The objective function of the FPA is to elevate entropy. This parameter is mathematically portrayed as depicted in the subsequent equation.

\[
En = -\sum_{j=1}^{n} p_{sj} \log_2 p_{sj}
\]  

(1)

Where, \( En \) denotes the entropy of the sequence, \( p_j \) indicates the ‘probability of occurrence of the \( sj^{th} \) sequence’ which is the count of possible states in every sequence.
Fig. 3. Flowchart of the FPA

The algorithm steps of the FPA that is requisite for the execution of the selection of a random key for the secured algorithm are as delineated here.

**Step 1:** Primarily, initialize a populace of \( n \) flowers with arbitrary solutions. The proposed system regards a population of keys that is delineated as,

\[
k_i = k_1, k_2, k_3, ..., k_n
\]  

(2)

**Step 2:** Ascertain the finest solution \( b \) in the primarily specified population.

**Step 3:** Delineate the switch probability \( p \) which is betwixt 0 and 1.
Step 4: When the maximal generation is not attained, the subsequent steps are executed. If the arbitrarily generated value is lesser on considering the switch probability, then execute the operations as of step 5 or else proceed from step 6.

Step 5: Draw a step vector $V$ which obeys a Levy distribution. Then global pollination is executed utilizing the subsequent mathematical delineation.

$$k_i^{t+1} = k_i^t + V(b - k_i^t) \quad (3)$$

Step 6: Draw $\beta$ as of a uniform distribution in $[0,1]$. The values $j$ and $k$ are picked in an arbitrary manner to form the solutions. The local pollination is executed utilizing the subsequent formula

$$k_i^{t+1} = k_i^t + \beta(k_j^t - k_i^t) \quad (4)$$

Step 7: The new solutions are appraised and it is contrasted to the former solution. If the new solutions are found to be better on considering the former solution, then it is updated in the population. This is the current finest solution. The new finest solution is indicated as

$$y_i = k_i^{t+1} \quad (5)$$

This algorithm is executed in the creation of key in the MAES algorithm. The finest value of the key is attained by utilizing the FPA. The finest key value that is attained as an outcome of the FPA has elevated value of randomness. For good understanding, the workflow of the FPA is delineated in fig 3.

III.iii. AES Encryption

The plaintext together with the key which is generated in the preceding step is utilized to make a CT. The CT is a scrambled edition of the original message/information. The CT safety greatly counts on the sort of key that is utilized in the algorithm. The algorithm which performs such sort of transformations on the PT is termed the encryption algorithms. In the MAES, the key which is provided as the input is after that expanded in to a collection of 44 32-bit words that is denoted as

$$u[i] = \{u[0], u[2]... u[43]\} \quad (6)$$

Fig. 4. Key and expanded key
Figure 4 gives the visual depiction of the key that is generated together with the expanded key. The MAES has a total of ten rounds. The initial nine rounds contain four stages namely, i) Byte substitution, ii) shift rows, iii) mix columns iv) add rounds key (ARK). The initial stage is used for permutation and also the other three stages are utilized for substitution. Figure 5 exhibits the operations that happen in round 1. The similar operations are done up to round 9. In the 10th round, byte substitution is not done; the other 3 stage is performed.

Fig. 5. A single rounds in encryption

The AES stands as an algorithm of the symmetric key that utilizes the same key to encrypt in addition decrypt a message. Moreover, the CT that is generated via this algorithm is of the same size as that of the PT one. The basic design principle of the AES stands as the substitutions-permutation network. The AES encryption can be described for a single round. Each round contains four sub-processes. The initial round is explained here.

III.iii.i. Byte Substitution

The AES states a 16X16 matrix of byte values termed as an S-box. This holds a permutation of all probable 256 8-bit values. Every byte of the state is mapped to a fresh byte on the subsequent way. The 4bits of the byte that is in the leftmost positions are utilized as row values together with the four bits that are present on the right-most value are utilized as the column value. These row & column values act as the index values on the S-box to choose the unique output.
III.iii.ii. Shift Rows

The forward shift row transformations are done in this step. The 1\textsuperscript{st} row of the state remains unaltered. For the 2\textsuperscript{nd} row, a one-byte circular left shift is done. Aimed at the 3\textsuperscript{rd} row, a 2-byte circular left shift is done. For the 4\textsuperscript{th} one, a 3-byte circulars left shift is executed. The in-verse shift rows transformation does the circulars shifts on the opposite directions.

III.iii.iii. Mix Columns

This process denotes the forwards mix columns transformation which functions on every column independently. Every byte of a column is mapped in to a fresh table which is the operation of the entire 4 bytes on that column. This transformation in a single column of a state can well be signified as below.
III.iii.iv. Add Round Key

The ARK denotes the forward ARK transformation. The sixteen bytes of the matrix is considered as 128 bits. These bits are XOR-ed with the 128 bits of the rounds key. Provided that this is the final rounds then the yield is the CT. Otherwise, the resultant 128 bits are deduced as 16 bytes and a new similar round begins.

This stage is the only stage that makes utilization of the key. Consequently, the cipher starts and also stops with an ARK stage. The end round of both the encryption & the decryption contains just three rounds.

III.iv. Decryption

Each stage that is done in encryption is reversible. This is also done in an easy manner. For the Byte Substitution, Shift Rows and also Mix Column stages, an inverse function is utilized on the decryption phase. In the MAES, the decryption algorithm makes utilization of the expanded key on the reverse order.
IV. Experimental Results

The proposed algorithm was simulated in the Java platform. The results that were obtained using the MAES was compared with the other cryptographic algorithms. The algorithms that were taken for the comparative scrutiny were the DES, Rivest Cipher (RC4) and Blowfish. Figure 10 denotes the file encryption time that is obtained for different files sizes in various algorithms.

It can be observed that as the file size increases, the encryption time sees an elevation in its values. The different files sizes that are taken for the analysis are 10,000 KB, 20,000KB, 30,000KB, 40,000 KB and 50,000 KB. The Blowfish algorithm takes the maximum time for encrypting a file with a specified file size. Conversely, the minimum encryption time is obtained using the MAES. This analysis displays the better performance of the proposed one on considering other security algorithms.

![Fig.10. File encryption time for different algorithms](image)

The decryption time is another essential criterion that is evaluated to ascertain the proposed work’s efficiency. Table 1 display the decryption time in milliseconds that is obtained for different file sizes in various algorithms that are taken for the analysis, on a tabular format.

**Table 1:** File decryption time for different algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time in milliseconds for different file sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10000 KB</td>
</tr>
<tr>
<td>MAES</td>
<td>2780</td>
</tr>
<tr>
<td>DES</td>
<td>3410</td>
</tr>
<tr>
<td>RC4</td>
<td>4100</td>
</tr>
<tr>
<td>Blowfish</td>
<td>5190</td>
</tr>
</tbody>
</table>

Security level stands as a gauge of the strength of a cryptographic algorithm. The proposed work’s security level can well be evaluated by means of ascertaining the


*M. Indrasena Reddy et al.*
percentage of attack that occur when various algorithms are employed. The MAES is less prone to attack on considering the DES, RC4 and the Blowfish. The Blowfish algorithm is highly susceptible to attacks. This scenario is exhibited in figure 11.

![Security Level Graph](image1)

Fig. 11. Comparative analysis of the security level.

The CPU memory utilization for different file sizes is analyzed. This analysis is extended to the other existent algorithms. The reduction in the memory usage is vital to prove the algorithm’s effectiveness. Memory usage during encryption using the MAES algorithm is found to be lower than the memory utilization of the other algorithms as perceived in figure 12.

![Memory Usage Graph](image2)

Fig.12. Memory usage on File Encryption

Decryption stands as the process of transmuting the encrypted text back in to its original text. The memory utilization for file decryption can be analyzed by using the values that are tabulated in Table 2. The MAES provides the better CPU usage when contrasted to the existing algorithms.
V. Conclusion

This paper dealt with the advancement of a secure approach for data transmission via computer networks. The MAES algorithm was developed as an enhancement to the traditional AES. The generation of the key in the MAES algorithm was done using the FPA. This improved the randomness of the process of producing the key aimed at encryption along with decryption. The MAES algorithm encompasses outstanding results when contrasting to the other existent algorithms. From the experimental results, it is evident that the encryption time, decryption time, memory usage and security level have yielded promising results. This justifies the MAES algorithm’s performance. This work can be further extended for diverse applications.

References


