SECURED COMMUNICATION IN WIRELESS NETWORKS USING MODIFIED ADVANCED ENCRYPTION STANDARD ALGORITHM

Mr. K Ravi Kumar[1], Karumanchi Ajay Babu[2], Narsing Chinna Sai Prasanth[3], Kanaparthy Muni Kumar[4],Chagarlamudi Yaswanth Simha[5]

[1] *Associate Professor, Dept. of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India*
[2] *UG Student, Dept. of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India*
[3] *UG Student, Dept. of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India*
[4] *UG Student, Dept. of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India*
[5] *UG Student, Dept. of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India*

ABSTRACT

In this work, the design and implementation of secure communication in the wireless network was carried out. The design was accomplished by using a Modified Advance Encryption Standard (MAES) algorithm and Intellij IDEA by Jetbrains. A byte rotation technique was used to modify the Advance encryption standard algorithm in order to improve security of files over a wireless network. In the work, files were encrypted such that if they fall in the hands of unauthorized users, their content remains secured because MAES was used to encrypt them. Text files of different sizes were used to test the design, and file encryption and decryption without loss in fidelity was achieved using the MAES algorithm A large number of text files of different sizes were used to test the system and the results obtained were compared with the Advanced Encryption Standard (AES) algorithm, which is also very efficient in terms of speed degree. Hence, byte rotation used to modify AES does not only improve security but equally little bit faster than AES. The research therefore recommend amongst other things the usage of MAES for securing files.

KEYWORDS *AES, Modified AES, Cryptography, wireless connection, Sockets, TCP/IP protocol, side channel attacks.*

1. INTRODUCTION

Information exchange has become a very important part of human life as it has become indispensable in daily activities. With the advent of technology, the exchange of information has become so easy and so efficient, that with the push of a button on phones, laptops and other communication devices, information can be Send, process and receive in no time at any destination. Within a certain distance where there is network coverage. With the increase in usage of these telecommunication systems and growth in internet technologies, there is also an increase in criminal

activities such as cyber thieves and hackers gaining access to vital data of their victims and sometimes using the same data to steal from them, impersonate them or for terrorism purposes. This is possible when the data transmitted are unsecured, and since the wireless network channel is the most widely used today, it is more exposed to cybercrimes. Therefore, there is need to secure sensitive data in such a way that they will appear senseless or meaningless to unauthorized users they are not intended for. To ensure this, data is encrypted into formats that are seemingly unreadable or corrupted to unauthorized people; this process is called cryptography.

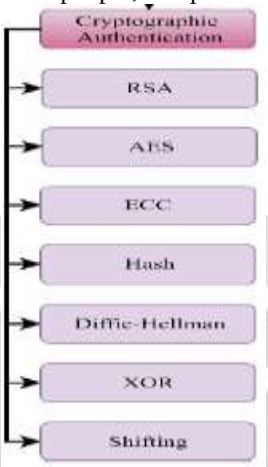


Fig 1: Types of Cryptographic Authentication

In cryptographic cycle, plaintext is the communication you are trying to transmit. That communication could anything that can be represented as a sluice of bits. The process of encryption converts that plaintext communication into cipher textbook, and decryption converts the cipher textbook back into plaintext. Encryption algorithms are technically classified in two broad orders; Symmetric crucial Cryptography and Asymmetric Key Cryptography. In symmetric type of Cryptography, the key that's used for encryption is same as the key used in decryption. Thus, the crucial distribution has to be made before transmission of any information.

2. ADVANCED ENCRYPTION STANDARD ALGORITHM

The AES encryption set of rules is a symmetric block cipher with a block/block length of 128 bits. It converts these individual blocks using 128, 192, and 256-bit keys. After encrypting these blocks, it combines them to form cipher text. It is based on the substitution permutation network, also known as the SP network. It includes a series of related operations, including replacing input with a specific output (substitution) and other operations involving rearranging bits (permutation). The essence of this research is to provide an effective means of securing files that are transmitted over a wireless network, such that intruders cannot gain access to the content of these files even if they lay their hands on them. This is possible because the files are encrypted using the Modified AES algorithm before they are transmitted, and are decrypted using the modified AES algorithm after they are received.

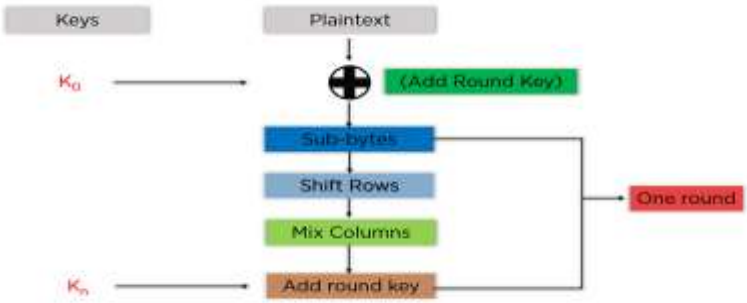


Fig 2: AES Flowchart

2.1 Attacks on AES

Research into attacks against AES encryption has continued since the standard was perfected in 2000.Many researchers have published attacks on low-cycle AES versions. In 2009, they discovered a possible critical attack. This cryptanalyst attempted to crack a cipher by studying how it works using different keys. The associated key attack was found to be a threat only to misconfigured AES systems.

A major threat to AES encryption comes from side- channel attacks. Rather than trying a brute- force assault, side-channel attacks are aimed at picking up blurted information from the system. Side- channel attacks, still, may reduce the number of possible combinations needed to attack AES with brute force. Side- channel attacks involve collecting information about what a computing device does when it's performing cryptographic operations and using that information to reverse- mastermind the device's cryptography system.

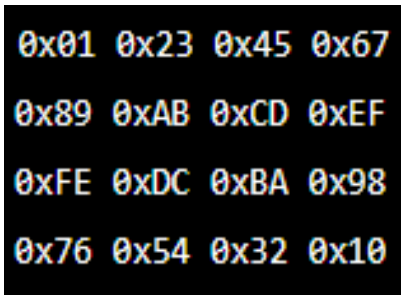
Now let's take the popular chat application whatsapp to explain the need of modification in the traditional AES algorithm.

Fig 3: Whatsapp

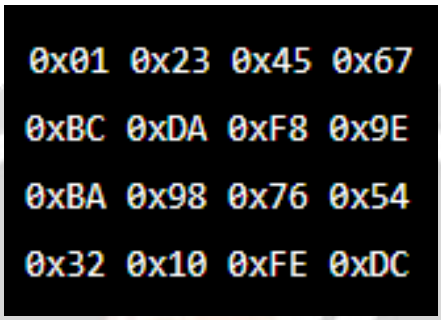
Whatsapp follows the AES encryption standard along with the combination of some other encryption algorithms. **AES-256/Curve25519/HMAC-SHA256** Even though Meta claims that it follows end-to-end encryption standards but we can find the traces of ours chats in other social media platforms and online shopping sites in the form of advertisements and recommendations. But all these comes under the company's privacy policy.
But there are some other illegal applications available which will take permissions from the users and breaks secured network to read the encrypted message. These apps will decrypt the received encrypted message from the receiver by applying the reverse engineering technique on AES algorithm. These are known as side channel attacks. In order to reduce these side channel attacks we some modifications in traditional AES algorithm as shown below.

2.2 Improving Security

In order to improve the security in the existing AES algorithm we are trying to modify the algorithm by adding an additional Byte Rotation step to it. Advanced Encryption Standard (AES) algorithm with an additional byte rotation step. AES is a symmetric encryption algorithm that is widely used in various applications, such as securing data transmission and storage. It uses a block cipher with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
The additional byte rotation step is an extension to the AES algorithm that adds an extra layer of security. In this step, each byte in the block is rotated to the left by a specific number of bits, depending on the position of the byte in the block. This rotation is performed after each round of encryption, which ensures that the output of each round is different from the input, making it harder for an attacker to decrypt the data. The byte rotation step involves shifting the bytes of each row in the block by a fixed number of positions to the left. The number of positions to shift each row is determined by the row number, with the first row being shifted by 0 positions, the second row by 1 position, the third row by 2 positions, and the fourth row by 3 positions. For example, if we have a block with the following 16 bytes:



After the byte rotation step, the block would look like this:



In this example, the first row is not shifted, the second row is shifted by one position to the left, the third row is shifted by two positions to the left, and the fourth row is shifted by three positions to the left.
The byte rotation step adds an extra layer of security to the AES algorithm because it makes it harder for an attacker to predict the output of each round of encryption. It also makes the algorithm more resistant to certain types of attacks, such as differential and linear cryptanalysis.
In conclusion, the AES algorithm with an additional byte rotation step is a secure and efficient encryption algorithm that can be used to protect sensitive data. The byte rotation step adds an extra layer of security to the algorithm and makes it more resistant to attacks. As such, it is a useful tool for protecting data in various applications.
After adding the additional byte rotation step this new modified algorithm is called Modified Advanced Encryption Standard Algorithm shortly MAES.

3. MODIFIED AES ALGORITHM

Here is a step-by-step explanation of the modified AES algorithm with an additional byte rotation step:

- Key Expansion: The first step is to expand the encryption key using the AES key expansion algorithm. The key expansion algorithm generates a set of round keys that will be used in the encryption process.
- Byte Substitution: In this step, each byte in the input block is substituted with a corresponding byte from a fixed lookup table called the S-box. This substitution is performed to make it harder for an attacker to recognize any patterns in the input data.
- Byte Rotation: This is the additional step that is added to the AES algorithm. In this step, each byte in the block is rotated to the left by a specific number of bits, depending on the position of the byte in the block. The number of positions to shift each row is determined by the row number, with the first row being shifted by 0 positions, the second row by 1 position, the third row by 2 positions, and the fourth row by 3 positions.
- Column Mixing: In this step, each column in the block is mixed using a matrix multiplication with a fixed matrix called the Mix Columns matrix. This mixing operation provides diffusion and confusion properties to the encryption algorithm.
- Round Key Addition: In this step, a round key generated during key expansion is added to the output of the previous step. This step ensures that each round of encryption produces a different output.
- Repeat Steps 2-5: Steps 2-5 are repeated for a fixed number of rounds, which depends on the key size used in the encryption. For a 128-bit key, the algorithm uses 10 rounds, for a 192-bit key, it uses 12 rounds, and for a 256-bit key, it uses 14 rounds.

- Final Round: In the final round of encryption, the byte rotation step is skipped, and the column mixing step is replaced with a simplified version called the InvMixColumns step. The InvMixColumns step is the inverse of the MixColumns step used in previous rounds.
- Output: The final output of the encryption algorithm is the encrypted block.

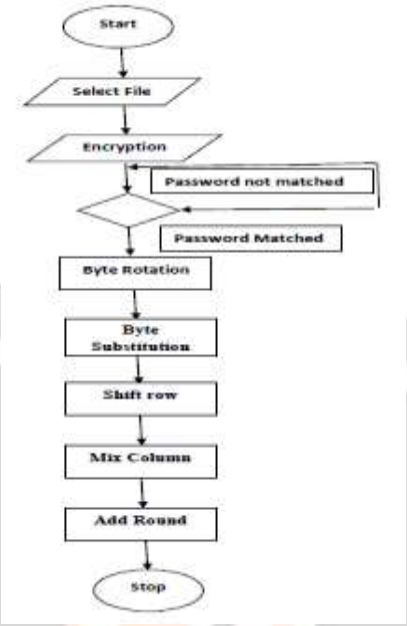


Fig 4: MAES Flowchart

The decryption process for the modified AES algorithm with an additional byte rotation step is similar to the encryption process, but the steps are performed in reverse order. The decryption process involves the use of a set of round keys generated during key expansion, which are used in reverse order to undo the effects of the encryption process.
Overall, the modified AES algorithm with an additional byte rotation step provides an extra layer of security and makes the encryption algorithm more resistant to certain types of attacks, such as differential and linear cryptanalysis.

3.1 System Implementation

The file encryption process will be done at the sender and decryption process will be done at the receiver following the MAES algorithm. The encrypted file from the sender to the receiver will be done by establishing the connection between the sender and the receiver by using the java socket programming as follows:

- Server Setup
- Client Connection
- Encryption of the file
- File Transfer
- Decrypting and reading the content
- Connection Termination

This is how the process follows.

4. RESULTS

4.1 Client Side

The input was taken in the form of the message by the text encryptor which follows the MAES algorithm to encrypt the message and saves the encrypted message in the file format

```
Input message :
This is a secret message.
Text message encrypted and saved to file.
```

Fig 5: Encryptor Output

This file was transferred from the client side to server side through a tcp/IP connection by taking the client authorization.

Fig 6: File Sender

Then the receiver will receive the file as

Fig 7: File Receiver

Now the receiver has to download the file file to decrypt it in order to see the content.

Fig 8: File Downloader

Finally the decryption process takes place and it works in the exact opposite way of text encryptor using the same key and also follows the MAES algorithm in order to view the encrypted message in the file received.

```
"C:\Program Files\Java\jdk-17\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2022.3.2\lib\idea_
.jar=9692:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2022.3.2\bin" -Dfile.encoding=UTF-8 -classpath
C:\Users\ajayk\IdeaProjects\AES\out\production\AES TextDecryptor
Decrypted message: This is a secret message.

Process finished with exit code 0
```

Fig 9: Decryptor Output

5. CONCLUSIONS

The purpose of the this work was to design a system that can perform secure communication via wireless network without interference by third party. If by any means the system is bypassed by unauthorized users, they will not be able to access the contents of the original message because the message is secured. Modified AES was realized via this system, which can encrypt binary files and decrypt them.Compared with the existing AES, the modified AES provides additional security by addition of byte rotation.

6. REFERENCES

[1] Jiang, Zilong; Jin, Chenhui; Wang, Zebin (2019). Multiple Impossible Differentials Attack on AES-192. IEEEAccess,7(),138011–138017. https:// doi.org/10.1109/access.2019.2942960

[2] J. Lu, O. Dunkelman, N. Keller, and J. Kim, ``New impossible differential attacks on AES," in *Proc. Int. Conf. Cryptol. India*, Dec. 2008, pp. 279_293.

[3] Sotirios Katsikeas, “Research communities in cyber security: A comprehensive literature review”,2021, https://doi.org/10.1016/j.cosrev.2021.100431

[4] Ritambhara,; Gupta, Alka; Jaiswal, Manjit (2017). [IEEE 2017 International Conference on Computing, Communication and Automation (ICCCA)- Greater Noida (2017.5.5-2017.5.6)] 2017 International Conference on Computing,Communication and Automation (ICCCA) - An enhanced AES algorithm using

cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT). , (), 422–427. doi:10.1109/CCAA.2017.8229877

[5] Bai, Kunpeng; Wu, Chuankun (2016). An AES-Like Cipher and Its White-Box Implementation. The Computer Journal, (), bxv119–. doi:10.1093/comjnl/bxv119

[6] Sruthis S. et al, "Encryption & Decryption of Text file and Audio using LabVIEW," 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum, 978-1-5090-6590-5/17/$31.00 ©2017 IEEE

[7]] Guy-Armand Yandji et al, "RESEARCH ON A NORMAL FILE ENCRYPTION AND DECRYPTION," 978-1-4244-9283-1/11/$26.00 ©2011 IEEE

[8] Biao Wei et al, "A Practical One-time File Encryption Protocol for IoT Devices," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 978-1-5386-3221-5/17 $31.00 © 2017 IEEE