IMPROVING AES ALGORITHM

Minor Project Work Summary Sheet

Enrol. No. (s) - 20104013, 20104025, 20104059

Name of Student (s)- Harshit Chopra, Kartik Gupta, Ayush Sharma

Name of supervisor - Dr. Shardha Porwal

May - 2023

Submitted in partial fulfilment of the Degree of

Bachelor of Technology

in

Information Technology

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY, NOIDA

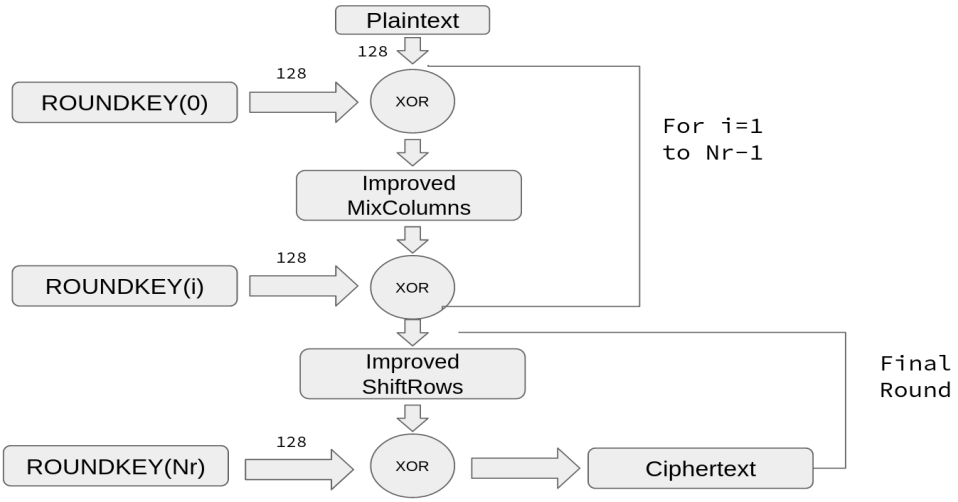
MOTIVATION BEHIND THE PROJECT

Cryptography, which is concerned with the study of techniques and procedures for secure data, is a component of information security. The most popular and commonly used symmetric cryptosystem is called Advanced Encryption Standard (AES). Our objective is to improve the AES algorithm.

TYPE OF PROJECT

Research cum development project.

OVERALL DESIGN OF PROJECT



1.Sub Bytes -Transformation process for a non-linear byte substitution using S.box lookup table

2. Shift Rows - Cyclical shifting process for key matrix in each row

3. Mix Column - Dot matrix operation combined with XOR using matrix finite field GF(2^8) and Galois Field.

4. Add Round Key - XOR addition operation for round key with state data

SubBytes: By employing Rijndael's S.Box lookup table, SubBytes are steps of byte-to-byte substitution. The table is 16x16 in size and includes hexadecimal characters in it. A given input key state byte is replaced by the hexadecimal.

A **Shift Row** is arranging the components of a state key matrix that shifts each row in a cyclical fashion. In each row, the circular shift length varies. Never is the front row relocated. The last element in the second row shifts the first element one space to the right. The last row moves three first components, and the third row moves two first elements to the right at the last element.

Mix Column is a linear process of change. Each state character element was multiplied by the coefficient element of GF(2^8). in the multiplication matrix that was created from two four-term polynomials.

We have made improvement in the shift row transformation by using array shift mapping instead of moving and rotating each element. We have also improved the Mix Column transformation process by combining different transformations into one and making the Sub Byte step unnecessary. The AES S-box has algebraic degree 254 with only 9 monomials which is very simple. We created a new affine transformation which increased the security of S-box. 256 is the unique period so that the distribution of elements of $F2^8$ is more balanced for the periodicity criterion. The algebraic complexity of the new S-box is 255, which is optimal and makes it more resistant to possible algebraic attacks than the AES S-box.

FEATURES BUILD, LANGUAGE USED

The reduction of the shift row circular procedure and the modification of the S.box for the transformation of the Mix Column are improvements. Combining Mix Column with a modified S.Box eliminates the need for the subbyte process.

Language used : C++

PROPOSED METHODOLOGY

- Instead of shifting and rotating each element, use array shift mapping to improve the shift row transformation.

- Mix Columns improvement by consolidating multiple transformations into one, the column transformation procedure eliminates the need for the Sub Byte phase.

- The AES S-box is fairly straightforward and has an algebraic degree of 254 with only 9 monomials. We developed a new affine transformation that improved S-box security. Since 256 is the only period, the distribution of $F2^8$ elements is more evenly distributed for the periodicity criteria. The new S-box is more resistant to potential algebraic attacks than the AES S-box since it has an ideal algebraic complexity of 255.

ALGORITHM/DESCRIPTION OF THE WORK

- Shift row steps involve a circular movement procedure that moves slowly. It can be enhanced, and the execution time can be shortened.
- A linear transformation procedure is Mix Column. Different transformations can be combined into one to reduce extra steps and improve performance.
- S-box should be written as a polynomial with a high algebraic degree. For the periodicity condition, the elemental distribution ought to be more evenly distributed.

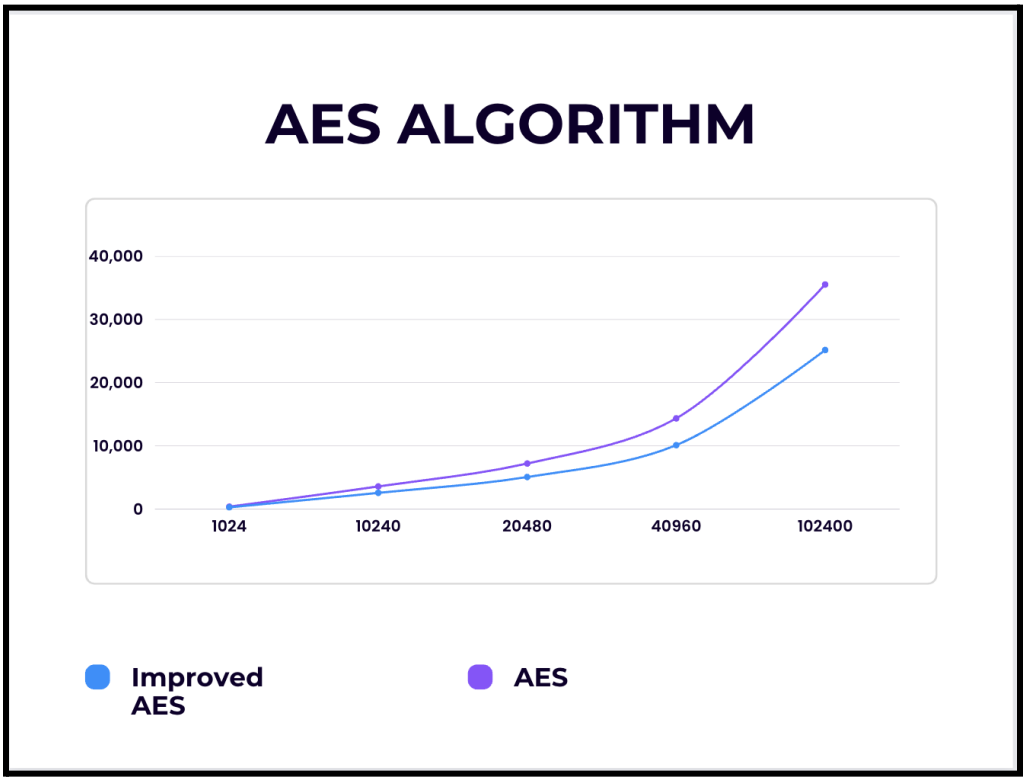
DIVISION OF THE WORK AMONG STUDENTS

Harshit Chopra: S-box security improvement.
Kartik Gupta: Shift Rows transformation with Result table and Graph.
Ayush Sharma: Mix Columns improvement.

RESULT

Advanced Encryption Standard has been successfully optimised. Our result shows that the percentage improvement on the encryption process is **34.4406%.**

Bytes	Normal AES(microsecond)	Improved AES(microsecond)
1024	360	253
10240	3565	2546
20480	7192	5053
40960	14340	10099
102400	35546	25168



CONCLUSION OF THE REPORT AND FUTURE SCOPE

The optimization of the Advanced Encryption Standard was successful. Array shift mapping has enhanced shift row transformation. The SubByte transformation step was eliminated by combining the Mix Column transformation stages into one. A new affine transformation improved the S-box's security. Since 256 is the only period, the distribution of $F2^8$ elements is more evenly distributed for the periodicity criteria. The new S-box is more resistant to potential algebraic attacks than the AES S-box since it has an ideal algebraic complexity of 255. According to our findings, the encryption process has improved by 34.4406%.

We can further improve the AES algorithm using following methods:

Use Hardware acceleration: Using specialist hardware, such as Field Programmable Gate Arrays (FPGAs) or Application-Specific Integrated Circuits (ASICs), the AES algorithm can be implemented.

Use Parallel Processing Methods: Utilise parallel processing techniques to implement the AES algorithm, which allows you to encrypt and decrypt data at the same time across several processor cores. The speed of computation can be considerably boosted by utilising more processing power.

Use SIMD Instructions: Utilising SIMD (Single Instruction Multiple Data) instructions, the AES algorithm can be improved. Multiple data elements can be processed simultaneously thanks to these instructions, which can speed up computation.