DISCRETE MINI PROJECT REPORT

CREATED BY:
1.ADITYA RAJ(2K19/CO/032)
2.ADITYA KUMAR SINGH (2K19/CO/031)

CONTENTS:

AIM

APPLICATION AND IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD(AES).

MOTIVATION

- **CRYPTOGRAPHY:** It is the practice and study of techniques for secure communication in the presence of third parties.It wasn't until the 19th century that it developed anything more than ad hoc approaches to either encryption or cryptanalysis.Mathematician Marian Rejeweski, at Poland's Cipher Bureau, in December 1932 deduced the detailed structure of the German Army Enigma, using mathematics and limited documentation.. In the UK, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient means for carrying out repetitious tasks.We are mainly influenced by Alan Turing for his work in decoding the enigma which led to the allied power winning the WWII .This culminated in the development of the Colossus, the world's first fully electronic, digital, programmable computer.

Cryptography has undergone many changes since then and so we wanted to understand the modern cryptography techniques and apply it to secure communication between two parties.

Our motivations in modern cryptography include:

1.Application of AES in cyber security

2.Securing end to end communication .

THEORY:

Cryptography involves the use of terms like plain text, cipher text, algorithm, key, encryption, and decryption. ‘Plain text’ is the text or message that needs to be transmitted to the intended recipients and which needs to be hidden. ‘Cipher text’ on the other hand, is the text that has been transformed by algorithms and which is gibberish.

The process of converting the information from ‘plain text’ to ‘cipher text’ is known as ‘encryption’. On similar lines, the process of converting ‘cipher text’ to ‘plain text’ is ‘decryption’.

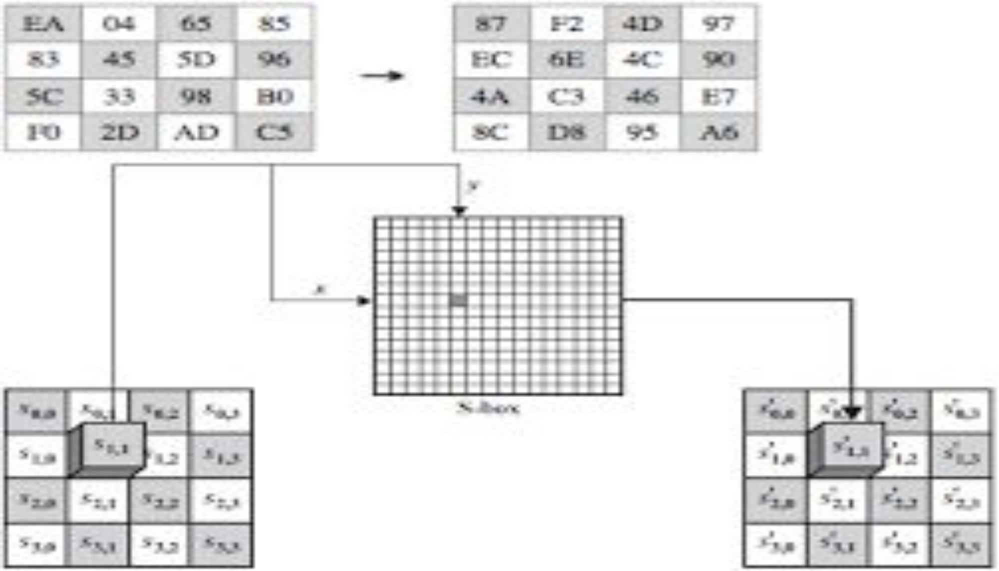
The complex mathematical formula that is used to convert ‘plain text’ to ‘cipher text’ is known as ‘algorithm’. Further, both the sender and the receiver have similar or different “keys” to encrypt and decrypt the message. A “key” is a “value that comprises a large sequence of random bits” . The larger the key size, the more difficult will it be to crack the algorithm. The “algorithm” and the “key” are the two important components of a cryptosystem.

AES ALGORITHM:

AES is based on a design principle known as a substitution -permutation network,, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network.It has a fixed text size of 128 bits but has a variant key size which depends on the number of rounds,10 rounds for 128-bit keys,12 rounds for 192-bit keys,14 rounds for 256-bit keys.AES operates on a 4 × 4 column major order array of bytes. AES algorithm uses a particular structure to encrypt data to provide the best security. To do that it relies on a number of rounds and inside each round comprise of four sub-process. Each round consists of the following four steps to encrypt 128 bit block :

1.SUBSTITUTE BYTES TRANSFORMATION:

The first stage of each round starts with SubBytes transformation. This stage depends on nonlinear S-box to substitute a byte in the state to another byte.



EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

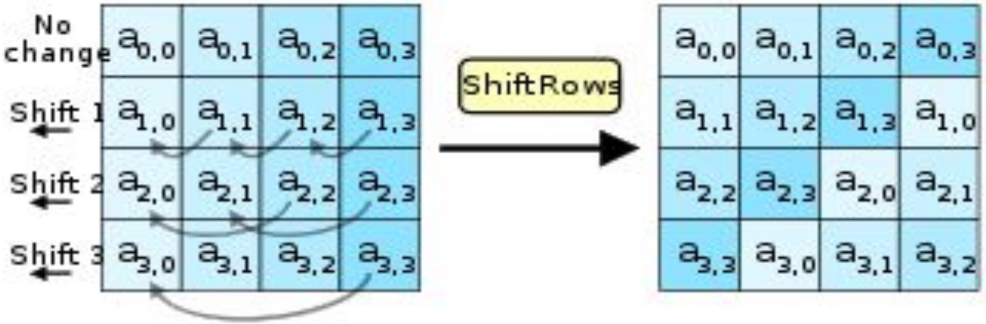
→

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

2.SHIFT ROWS TRANSFORMATION:

In this process the bytes of row number zero remains and does not carry out any permutation. In the first row only one byte is shifted circular to left. The second row is shifted two bytes to the left. The last row is shifted three bytes to the left

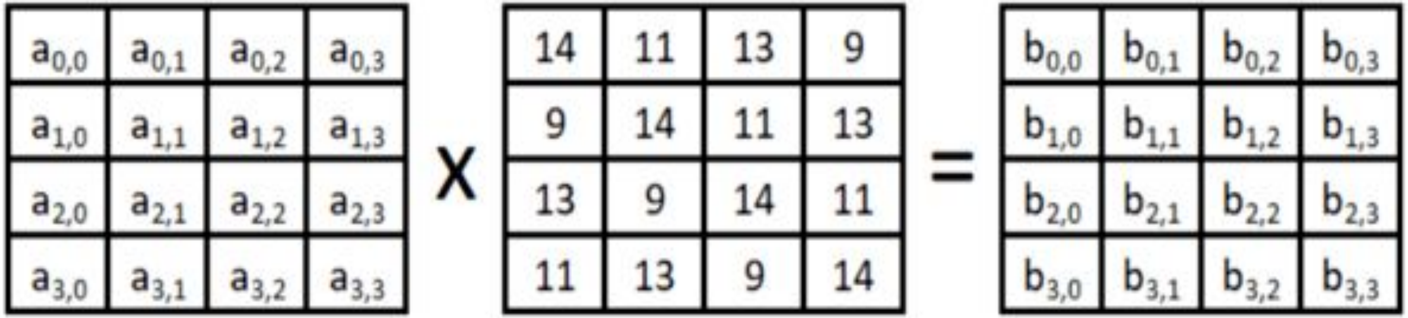


$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

3.MIX COLUMNS TRANSFORMATION:

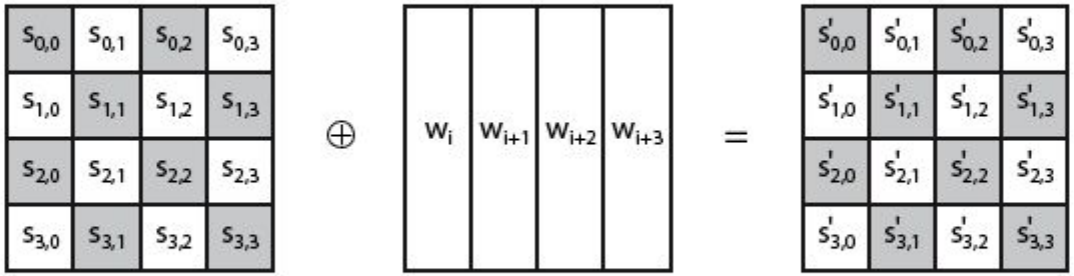
Each byte of one row in matrix transformation multiply by each value (byte) of the state column.The results of these multiplication are used with XOR to produce a new four bytes for the next state



$$\begin{array}{|c|c|c|c|}\hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \times \begin{array}{|c|c|c|c|}\hline 14 & 11 & 13 & 9 \\ \hline 9 & 14 & 11 & 13 \\ \hline 13 & 9 & 14 & 11 \\ \hline 11 & 13 & 9 & 14 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

4.ADD ROUND KEY TRANSFORMATION:

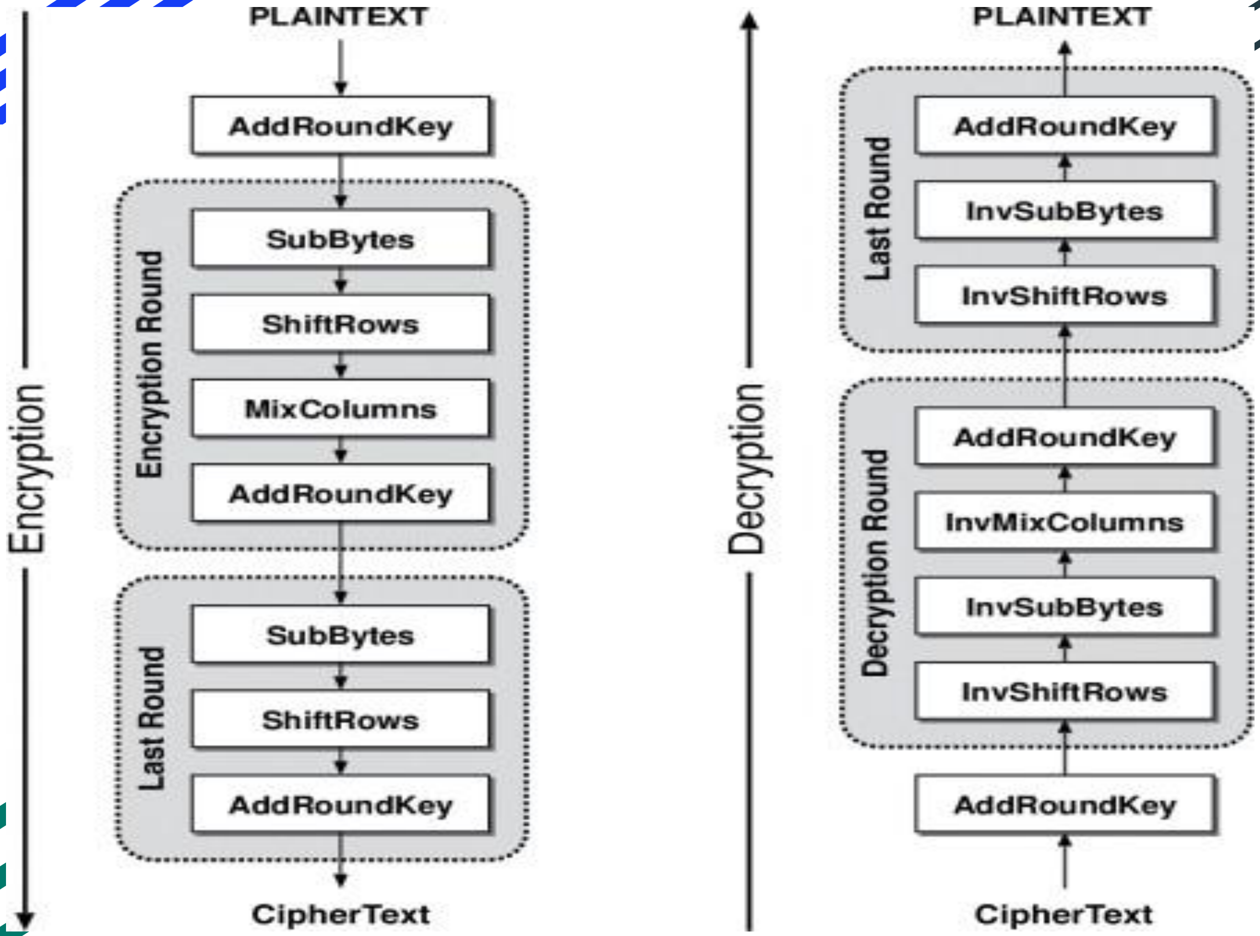
AddRoundKey is the most vital stage in AES algorithm. Both the key and the input data (also referred to as the state) are structured in a 4x4 matrix of bytes. It has the ability to provide much more security during encrypting data. This operation is based on creating the relationship between the key and the cipher text



$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \oplus \begin{bmatrix} w_i & w_{i+1} & w_{i+2} & w_{i+3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

KEY EXPANSION:

Each round has a new key.The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Where Nr is the number of rounds.The cipher key (initial key) is used to create the first four words. The size of key consists of 16 bytes


Encryption
PLAINTEXT
AddRoundKey
Encryption Round
SubBytes
ShiftRows
MixColumns
AddRoundKey
Last Round
SubBytes
ShiftRows
AddRoundKey
CipherText
Decryption
PLAINTEXT
Last Round
AddRoundKey
InvSubBytes
InvShiftRows
Decryption Round
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
AddRoundKey
CipherText

REAL LIFE APPLICATION

1) CYBER SECURITY

2) END-TO-END ENCRYPTION ON SOCIAL MEDIA PLATFORM

3) DIGITAL SIGNATURE

BIBLIOGRAPHY

- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

- https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data

- https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm