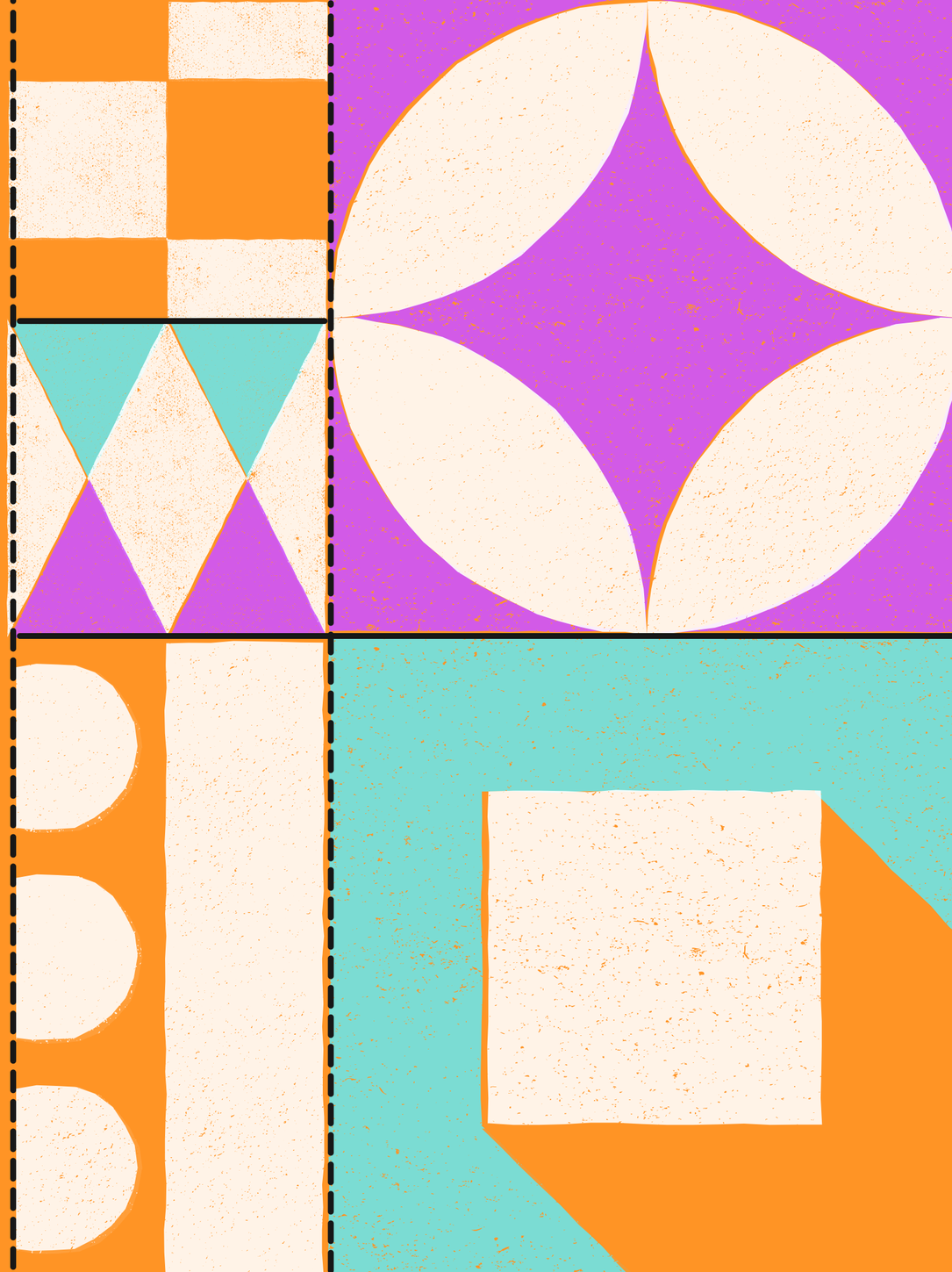
GITAM University

Advanced Encryption Standard

Samuel Vasamsetti - 121910315006

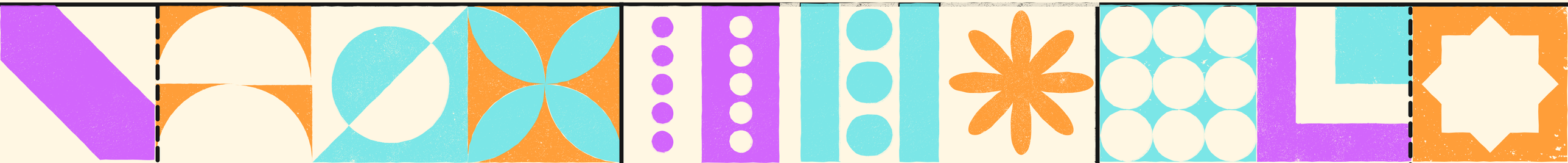
Cryptography & Network Security - 19ECS305



History of AES

Why AES? Who designed it?

Until the 2000s, triple DES was used for the encryption of data. DES has its own problems, attacks like Brute-force, Linear crypt-analysis, and Differential crypt-analysis are possible.
This lead to the need for an Advanced Encryption Standard. AES is based on Rijndael algorithm designed by Vincent Rijmen, Joan Daemen.



Rijndael

Serpent

Twofish

RC6

MARS

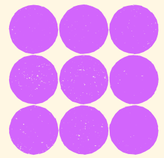
SHORTLISTED ALGORITHMS

Working of the Rijndael Algorithm

Unlike the DES algorithm, which is based on Feistel network, Rijndael (AES) Algorithm is based on S-P network.
AES is a 128-bit block cipher.
There are 4 transformations involved in this algorithm.

AES allows keys of sizes:

- 16 bytes (128-bit)
- 18 bytes (192-bit)
- 24 bytes (256-bit)

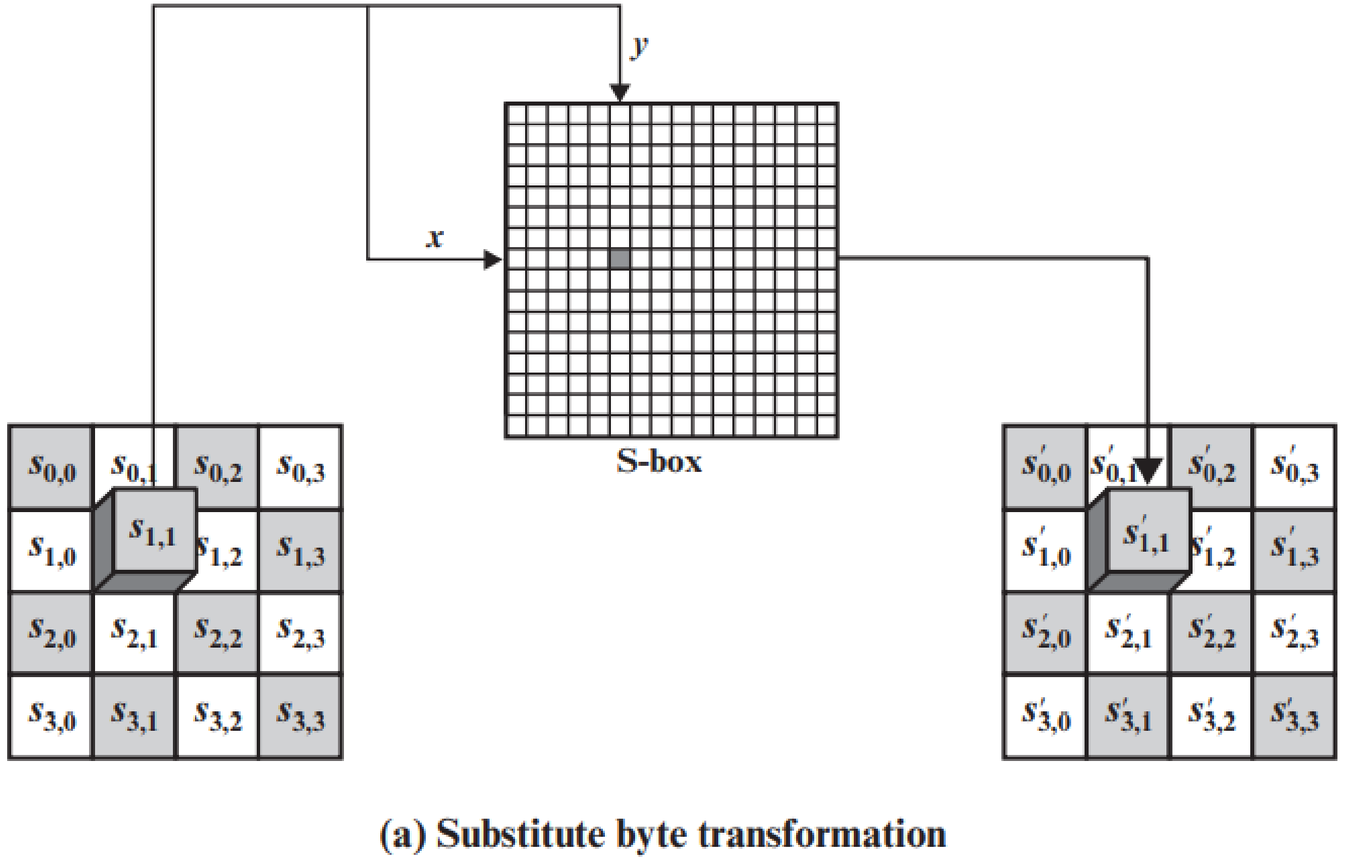


Substitute Bytes

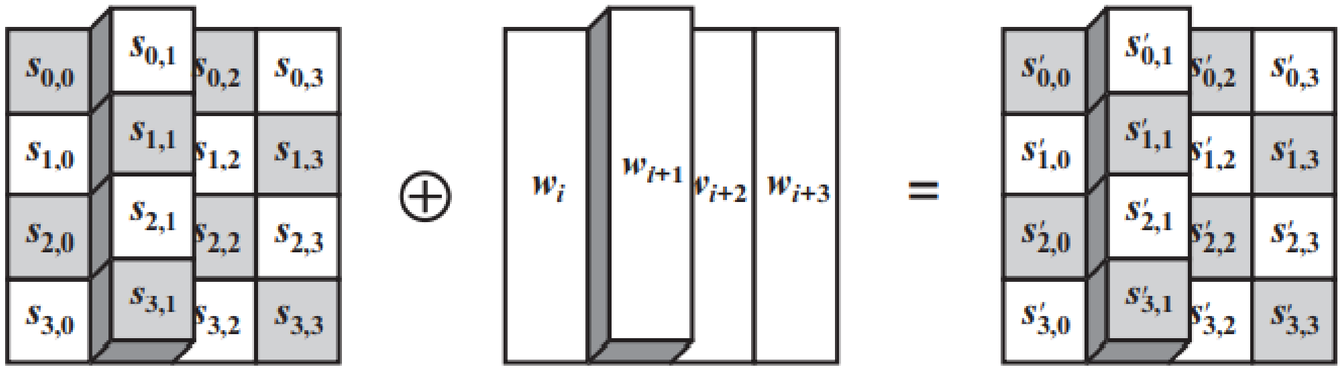
Shift Rows

Mix Columns

Add Round Key



(a) Substitute byte transformation

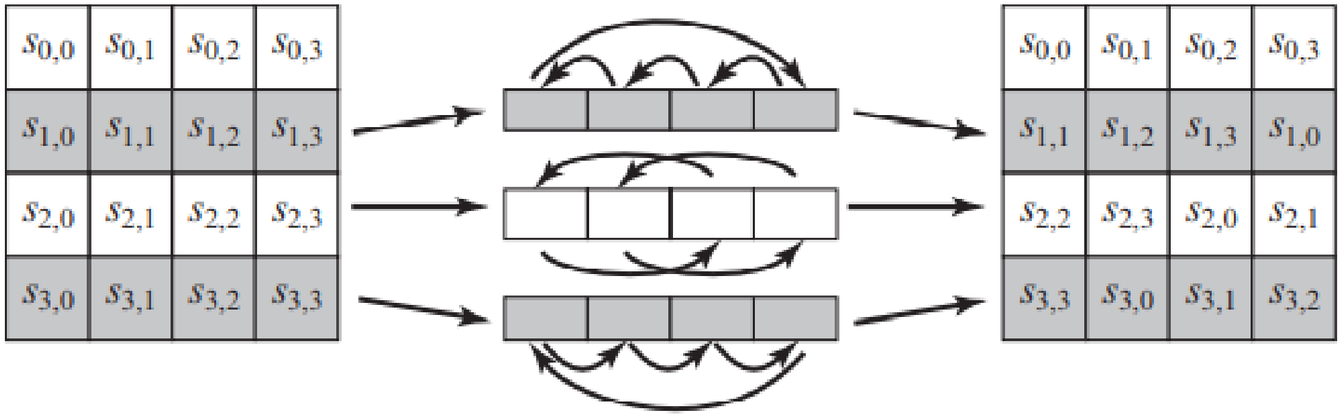


(b) Add round key transformation

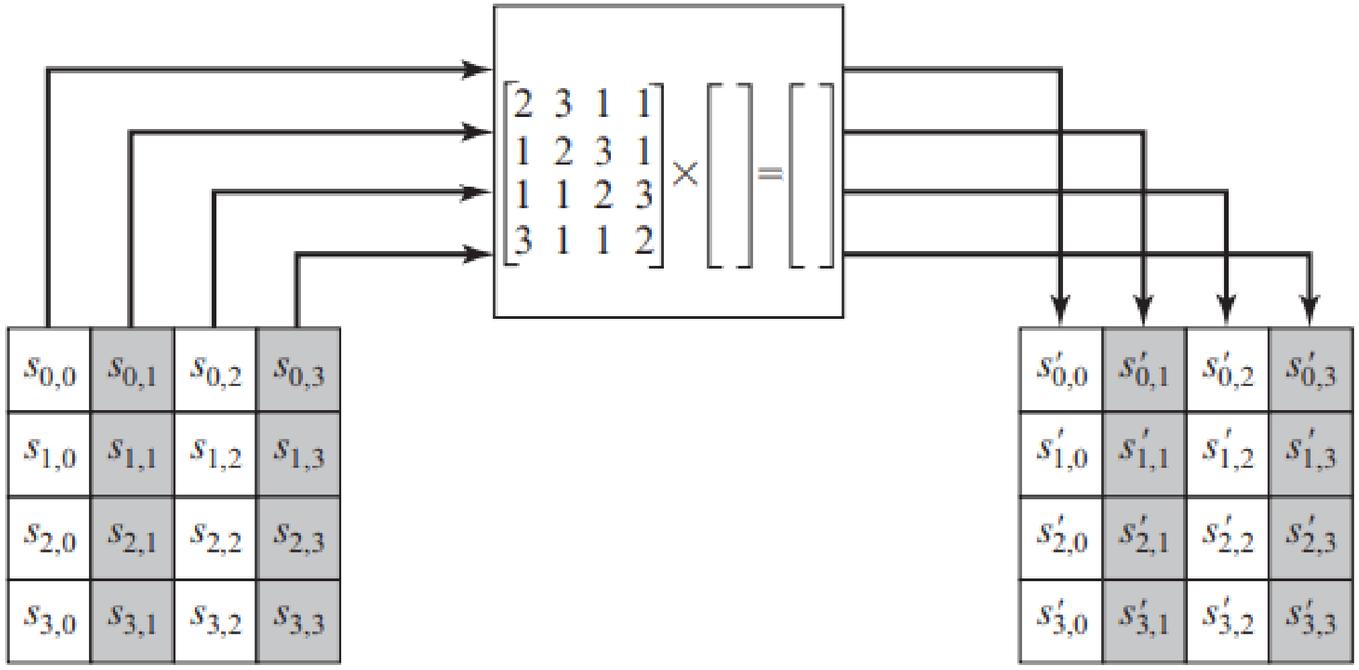
SubsBytes AddRoundKey

SubsBytes
Substitute values in s-box.

AddRoundKey
XOR the round key with the state matrix.



(a) Shift row transformation



(b) Mix column transformation

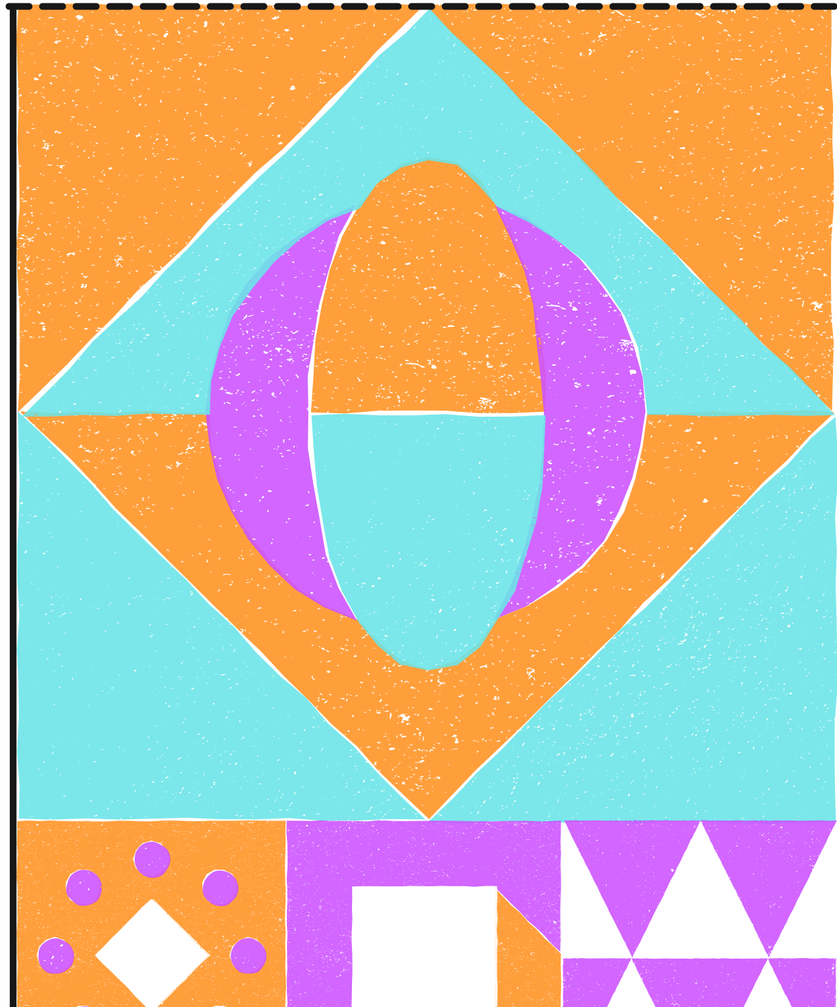
ShiftRows MixColumns

ShiftRows
Circular shift rows of the state matrix.

MixColumns
Matrix multiplication of a matrix with each column of state matrix is done.

Use XOR (⊕) instead of Plus (+),
Use Polynomial Reduction Modulo (·) for Multiply (×)

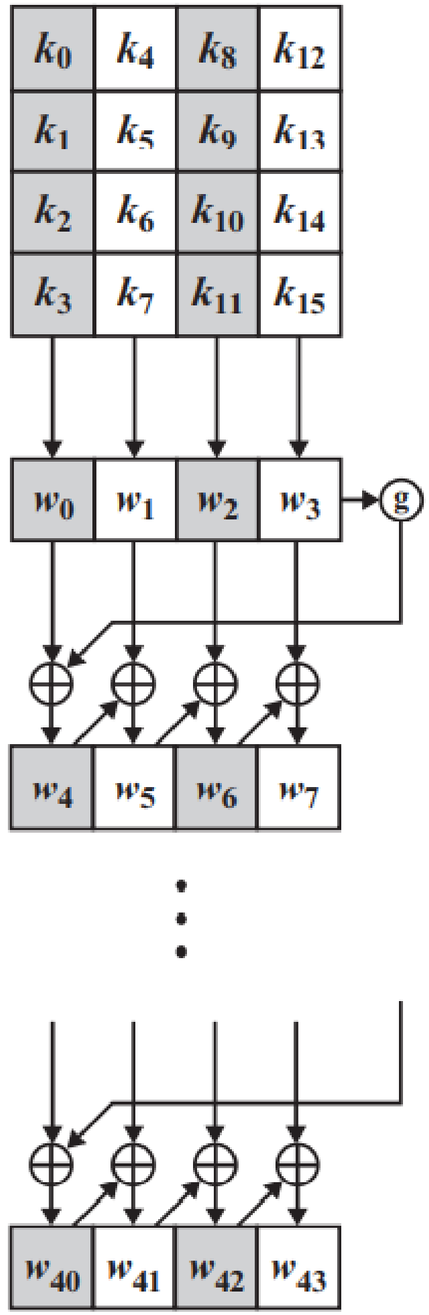
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$



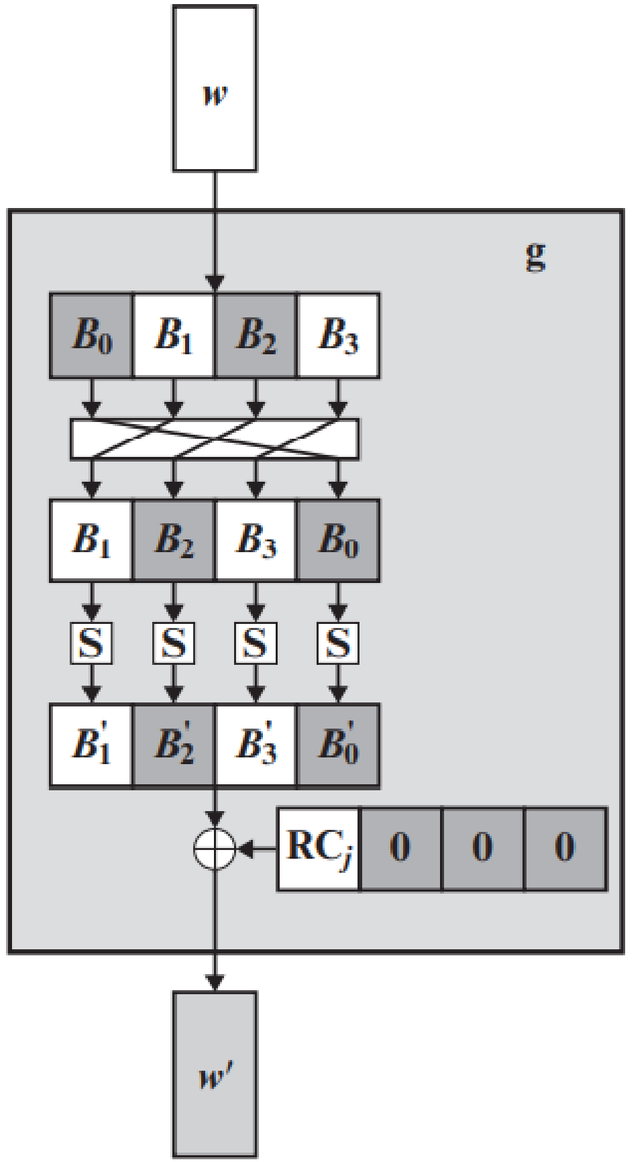
Key Expansion

The 16 bytes or 128-bit key is used to generate 44 words which we will use as round keys.

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36



(a) Overall algorithm

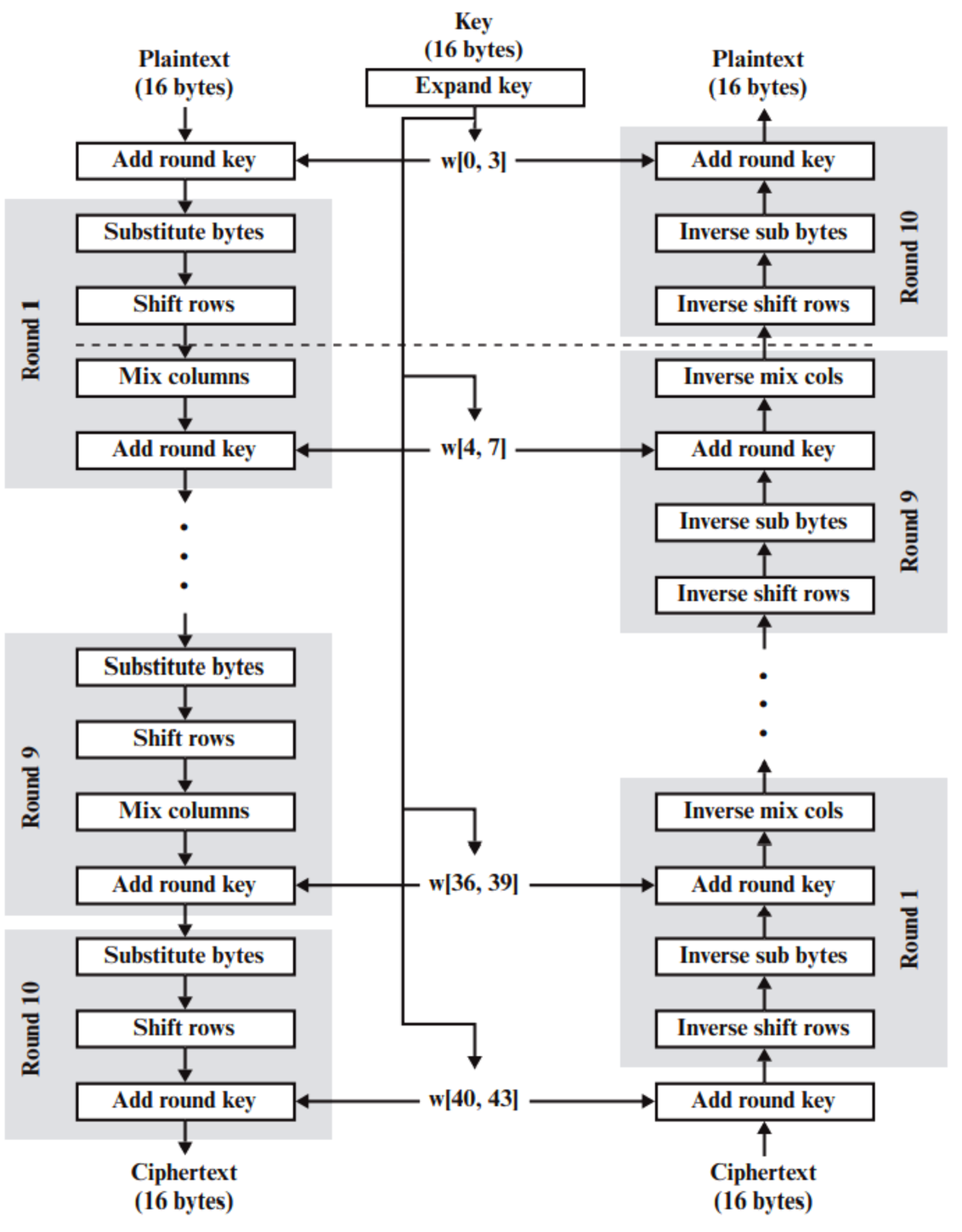


(b) Function g

The Process

This is the whole process of AES.

Live AES demonstration!



GITAM University

THE END

Samuel Vasamsetti - 121910315006

Cryptography & Network Security - 19ECS305