Cryptography

# Member

* Nguyễn Đăng Khoa – HE150820
* Phạm Thiên Nhật – HE150661
* Nguyễn Minh Tùng – HE150283
* Nguyễn Trần Nhật Bảo – HE150116

# Overview

## What is Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behaviour.

Cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages.

The assumption is that two entities wanting to communicate - Alice and Bob - are shouting their messages in a room full of people. Everyone can hear what they are saying. The goal of cryptography is to protect this communication so that only Alice and Bob can understand the content of the messages.

Modern cryptography is heavily based on mathematical theory and computer science practice.

Modern cryptography has many purposes:

* Confidentiality: only the intended recipient can decrypt the message and read its contents
* Authentication: the sender and recipient can verify each other’s identities and the destination of the message
* Integrity checking: Integrity focuses on the ability to be certain that the information contained within the message cannot be modified while in storage or transit
* Non-repudiation: the sender of the message cannot backtrack in the future and deny their reasons for sending or creating the message

## Types of Cryptography:

* Symmetric Key Cryptography: It is an encryption system where the sender and receiver use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange Key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
* Hash Functions: There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
* Asymmetric Key Cryptography: Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public Key and Private Key are different. Even if the public key is known by everyone, the intended receiver can only decode it because he alone knows the private key.

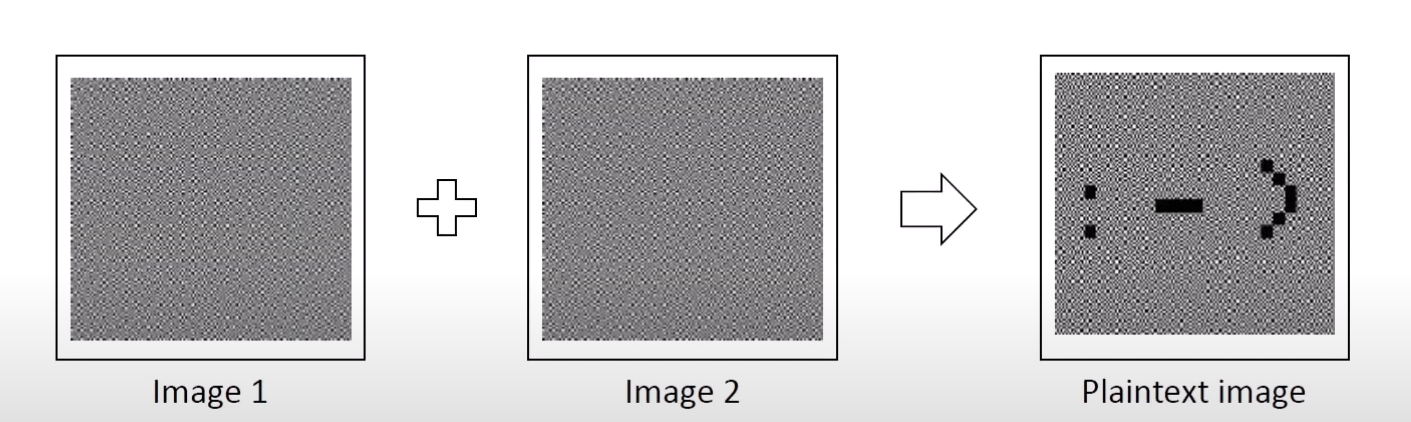
# Visual Secret Sharing

## Overview

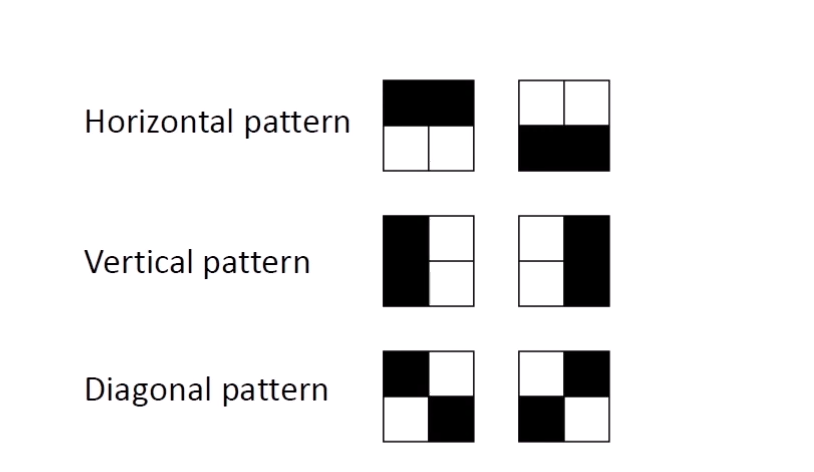
* Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image.
* In 1994, Naor and Shamir present a secret sharing method where an image is broken into n shares and any n - 1 shares are not enough to decrypt it.
* Using similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

## Encryption and Decryption

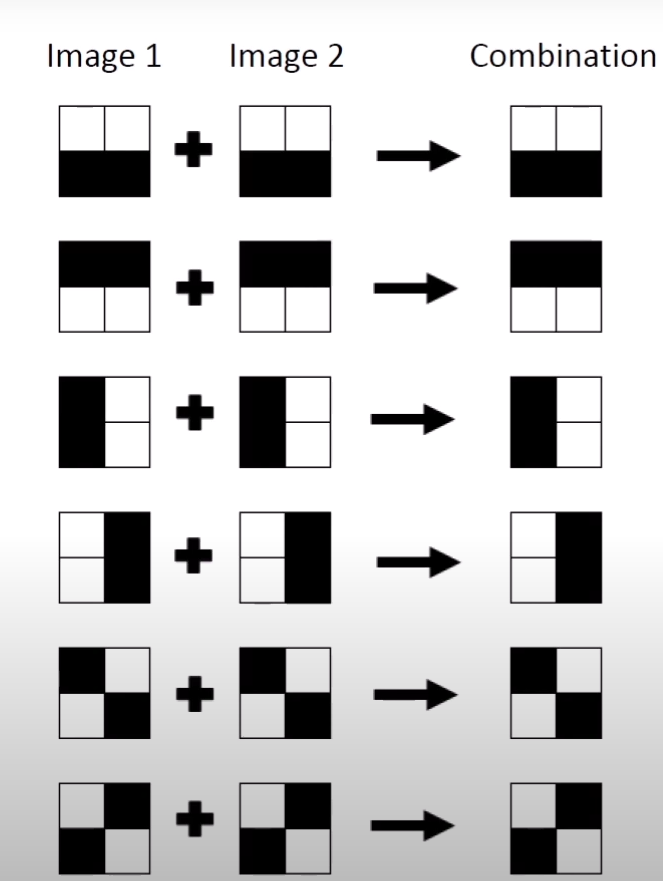
* We create one image **(Image 1)** which acts as shared one-time-pad and another image **(Image 2)** which is our **ciphertext**



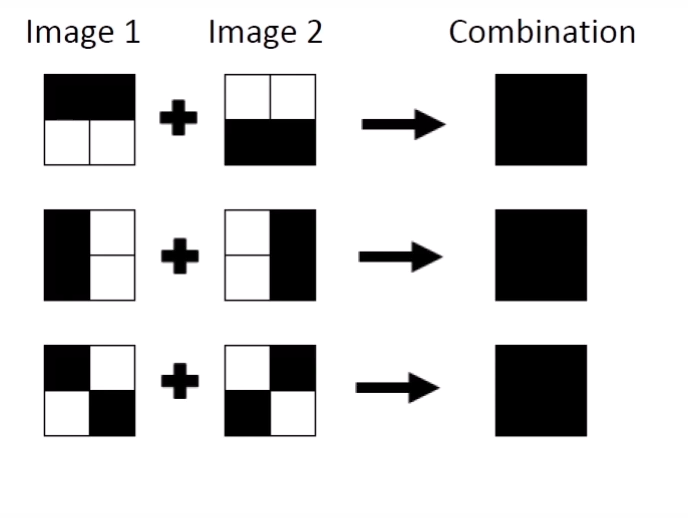
* When we combine **image 1** and **image 2**, we get our **plaintext image**.
* This work also by printing image 1 and image 2 on plastic sheets and overlaying these.
* Because we encrypt black & white image, we need to encrypt black and white pixels.
* We need different encryption pattern for encryption.
* We use three different 2x2 patterns as defined as follow:



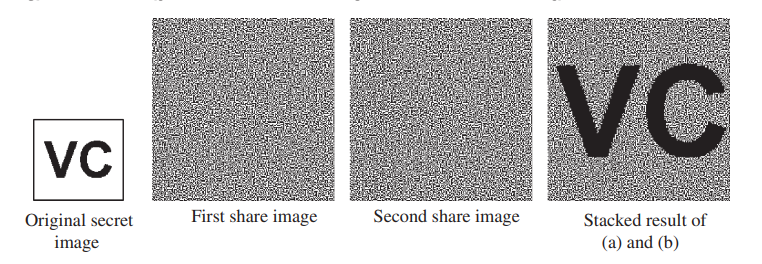
* For white pixel, we use for each image the same randomly chosen pattern



* As for black pixel, we use for each image a randomly chosen pattern and it inverse:



## Example



Here we shift and overlay two images (pad and ciphertext)

Only when both images are perfectly aligned, the secret message is visible.

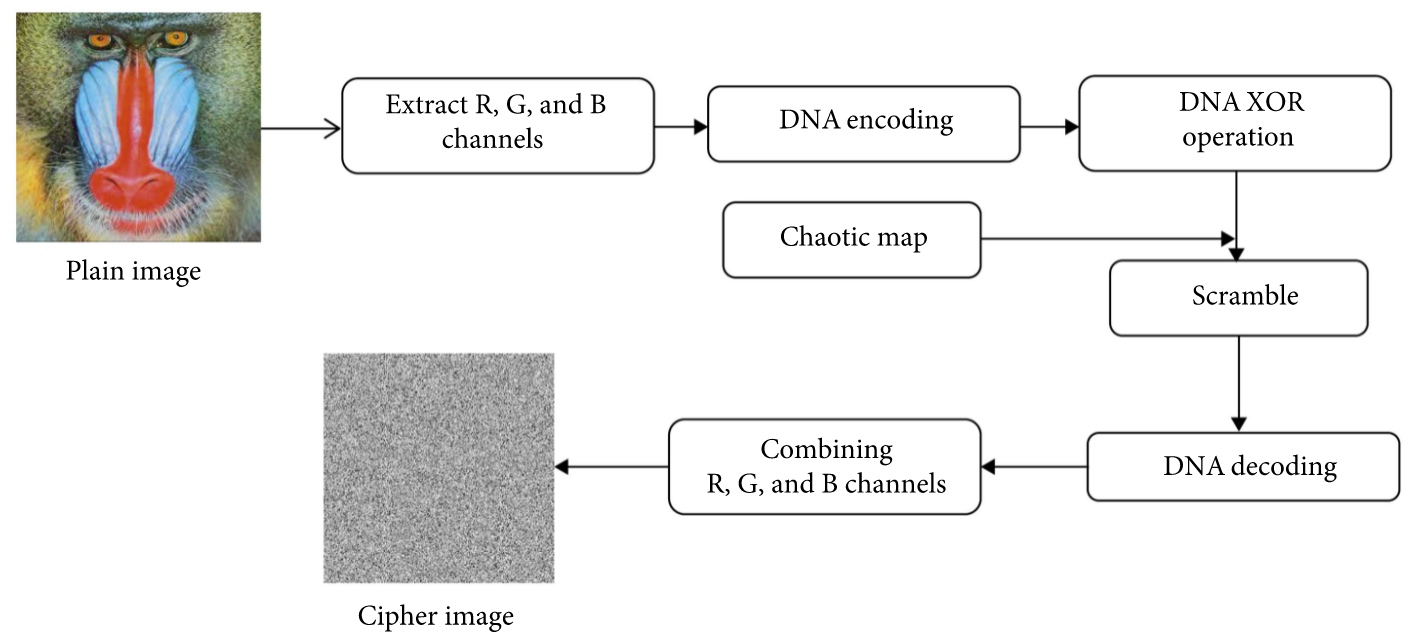
# DNA encoding

## Overview

* Deoxyribonucleic acid (DNA) cryptography has become very popular due to its properties such as massive parallelism, huge storage, and ultra-low power consumption.

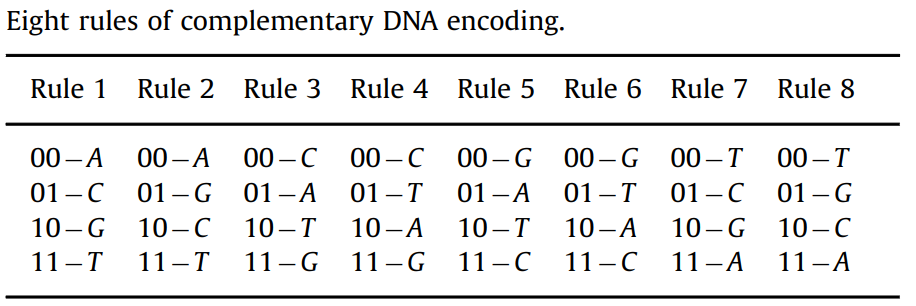
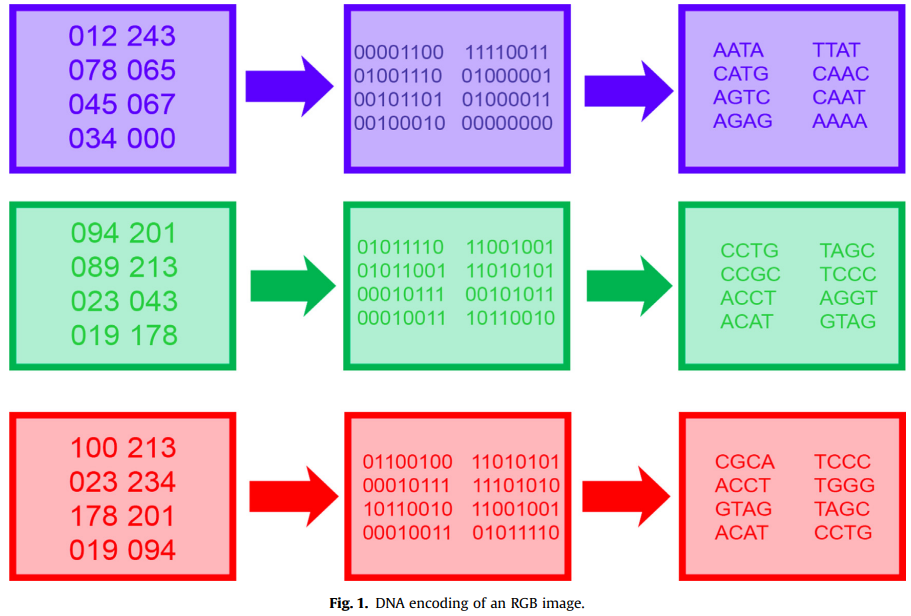
## Encryption and decryption

* The color image is decomposed into three channels red (R), blue (B), and green (G). After that, DNA encoding and XOR operations are utilized to encode the channels. A chaotic map can be utilized to scramble matrices. Finally, three R, G, and B channels are combined to obtain the cipher image



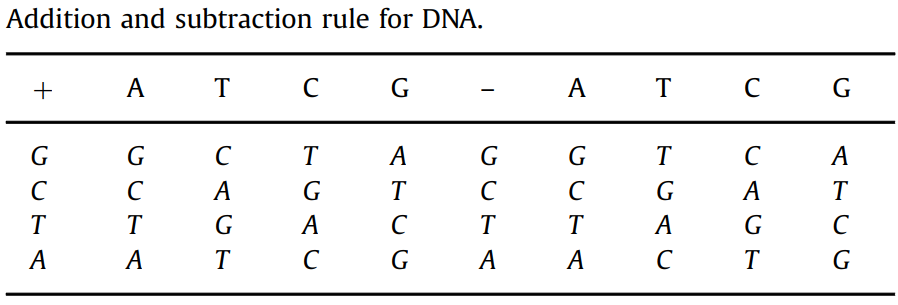
## DNA encoding

The value of the pixels is decomposed into binary numbers (m x (n x 8)), where m and n are row and column size, and is encoded into DNA using rule of complementary DNA encoding.

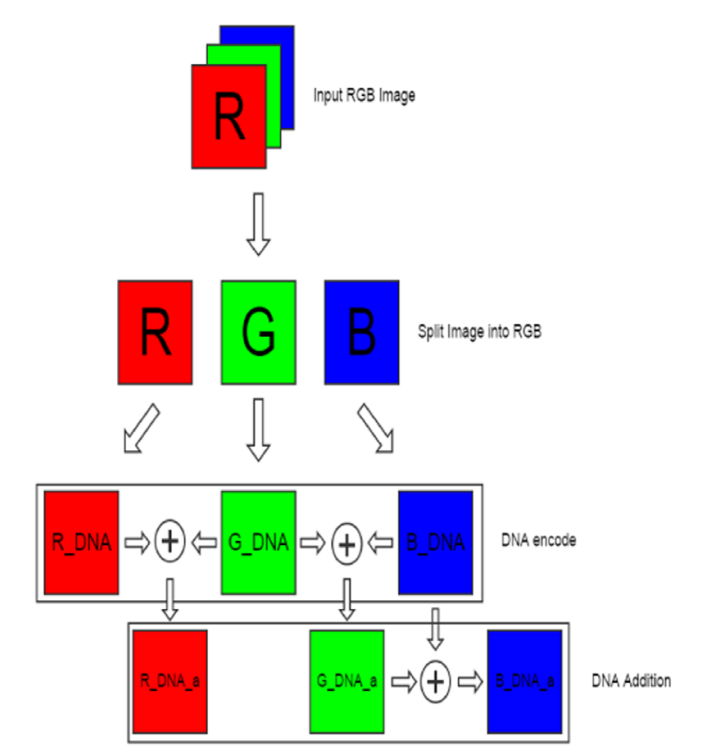


## XOR operation

* XOR operation is used to further scramble the image, by combining the DNA encoded matrixes to create a new one using addition and subtraction operation.



## Example



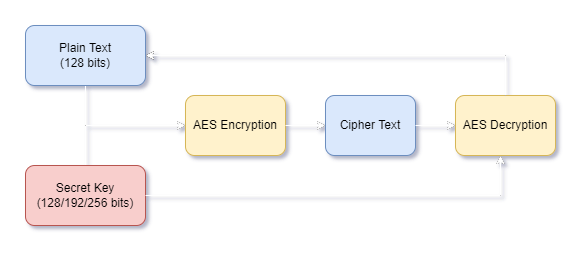
# Advance encryption standard

## Overview

* Advanced Encryption Standard, or AES, is a Rijndael block cipher-based encryption standard for digital data.
* developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.
* Is a symmetric key and symmetric block cipher, meaning the same key is used for both encrypting and decrypting the data.
* One of the cryptographic gold standards for securely encrypting and preventing unauthorized access to electronic data, still widely used as of today.

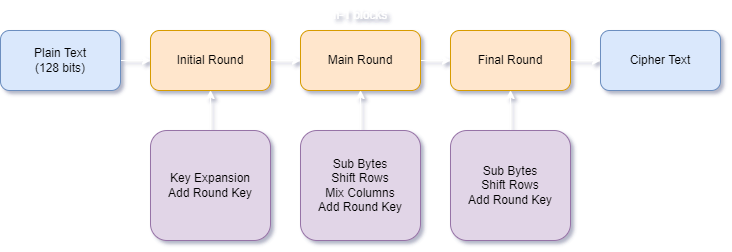
## How it works

The AES creates ciphertext, which is an unreadable, indecipherable conversion of plaintext data, which can only be read after the secret AES key is used to decrypt it.



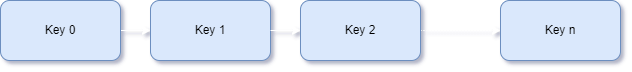
The key size used for an AES cipher specifies the number of transformations rounds that convert the input. The number of rounds is as follows:

* 10 rounds for 128-bit keys.
* 12 rounds for 192-bit keys.
* 14 rounds for 256-bit keys.



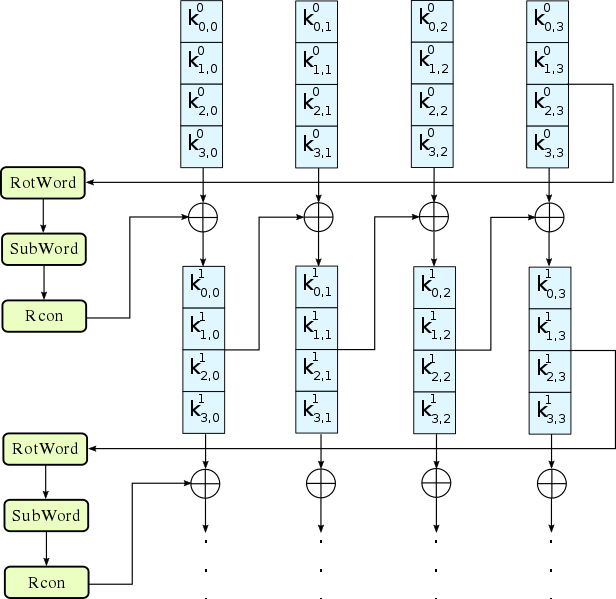
## Key Expansion

AES uses a separate key schedule to expand a short key into a number of separate round keys. With each variants having different number of rounds, the key schedule needs to produce the needed round keys for each round.



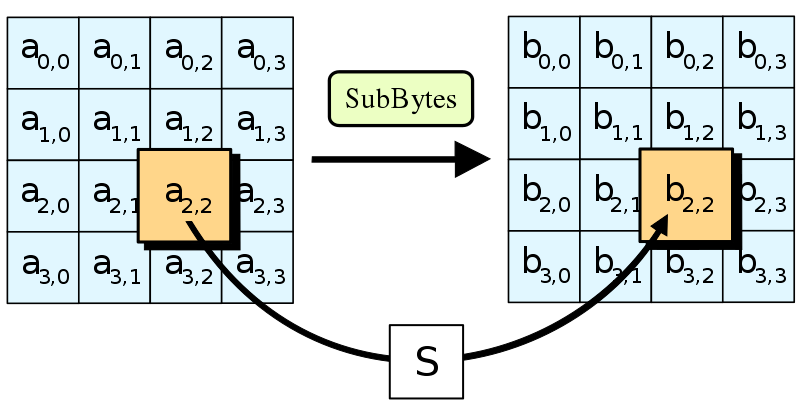
We can define the Key Schedule as a simple 3-stage process:

1. Perform Rot Word on the last column of key.
2. Perform Rot Word on the column.
3. XOR the column with RCON and then XOR with the i-th column of key.
4. Repeat 3 while iterating i, until i is equals to 3 (all 4 column of keys required).



## Sub Bytes

Sub Bytes means replacing each byte a(i, j) with the corresponding value in S-Box.

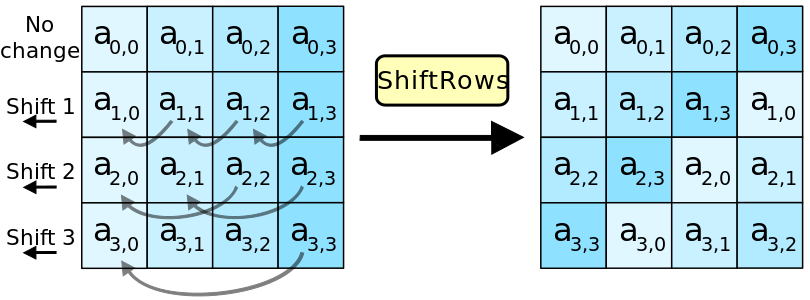


The Rijndael S-box used in AES maps an 8-bit input, c, to an 8-bit output, s = S(c). It is known to possess good non-linearity properties.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **00** | **01** | **02** | **03** | **04** | **05** | **06** | **07** | **08** | **09** | **0a** | **0b** | **0c** | **0d** | **0e** | **0f** |
| **00** | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| **10** | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| **20** | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| **30** | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| **40** | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| **50** | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| **60** | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| **70** | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| **80** | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| **90** | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| **a0** | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| **b0** | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| **c0** | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| **d0** | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| **e0** | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| **f0** | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

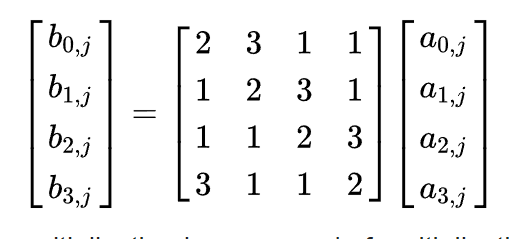
## Shift Rows

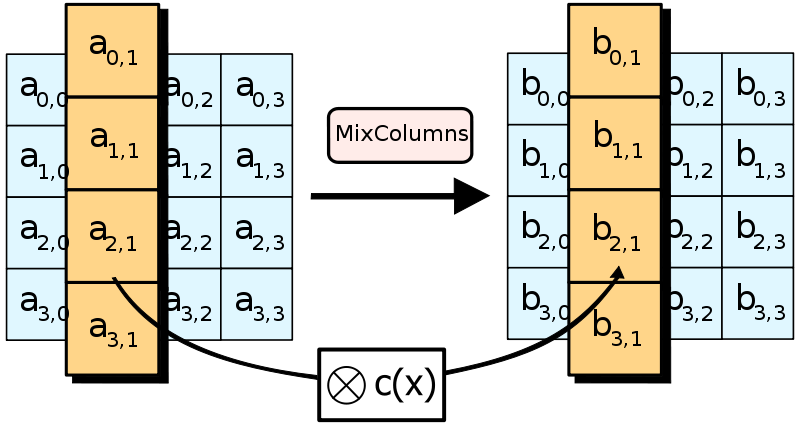
For the Shift Role stage, we will be left shifting, with the amount of shift increasing by 1 for each column we processed, from 0 to 3.



## Column Mix

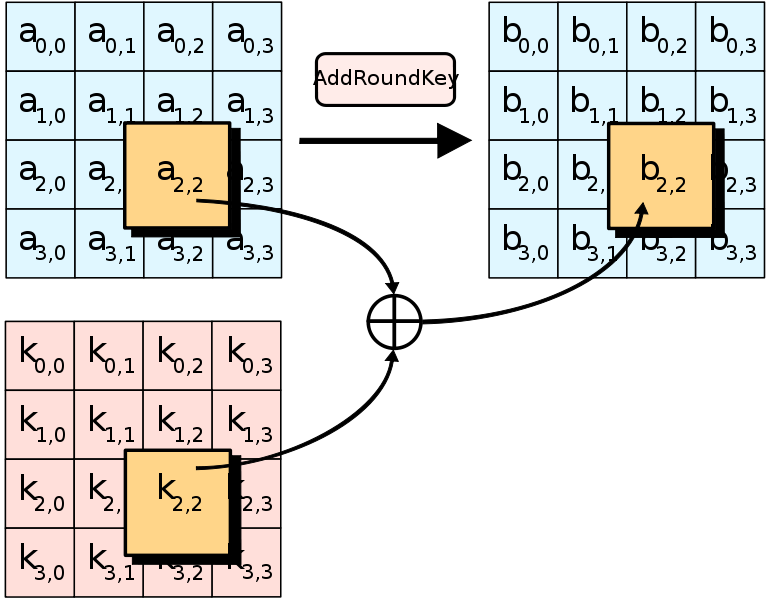
Column Mix is a linear mixing operation which operates on the columns of the state, combining the four bytes in each column. Its purpose is to provide diffusion in the cipher.





## Add Round Key

It’s simply a XOR between the data block and the round key.

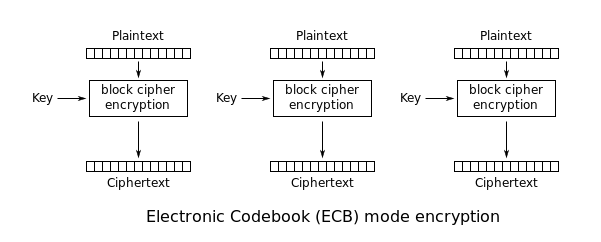


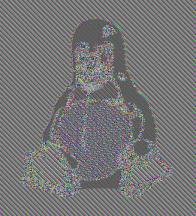
## Modes of operations

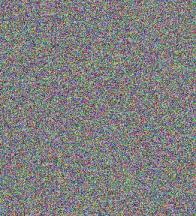
Normally, AES would only encrypt a 128-bit plain-text block of data, so for bigger data, we need to have a rule to apply AES. Modes of operation is made to regulate this problem, defining how each block would be encrypted in a large file.

There are many modes of operation, but the two most commonly used are:

* Electronic codebook (ECB)
* Cipher block chaining (CBC)

 Note that while ECB seems plausible, it’s not a very suitable one for encrypting data such as image, audio,… since these data have a “pattern” that can reoccur. In fact, if we grayscale an image and compare itself in two stages, we can see that the histogram still resembles themselves much.



To tackle this, we can just use any other mode of operation, here we have CBC for example, it’s known for being much more secure since if the (IV) fail to initialize, the data would barely even resemble the original data block at all. 

Basically we will just XOR each data block with the one before for each stage, starting with the IV.

