

# Secure Documents II: Simplified AES

1936-2 ANOS IF



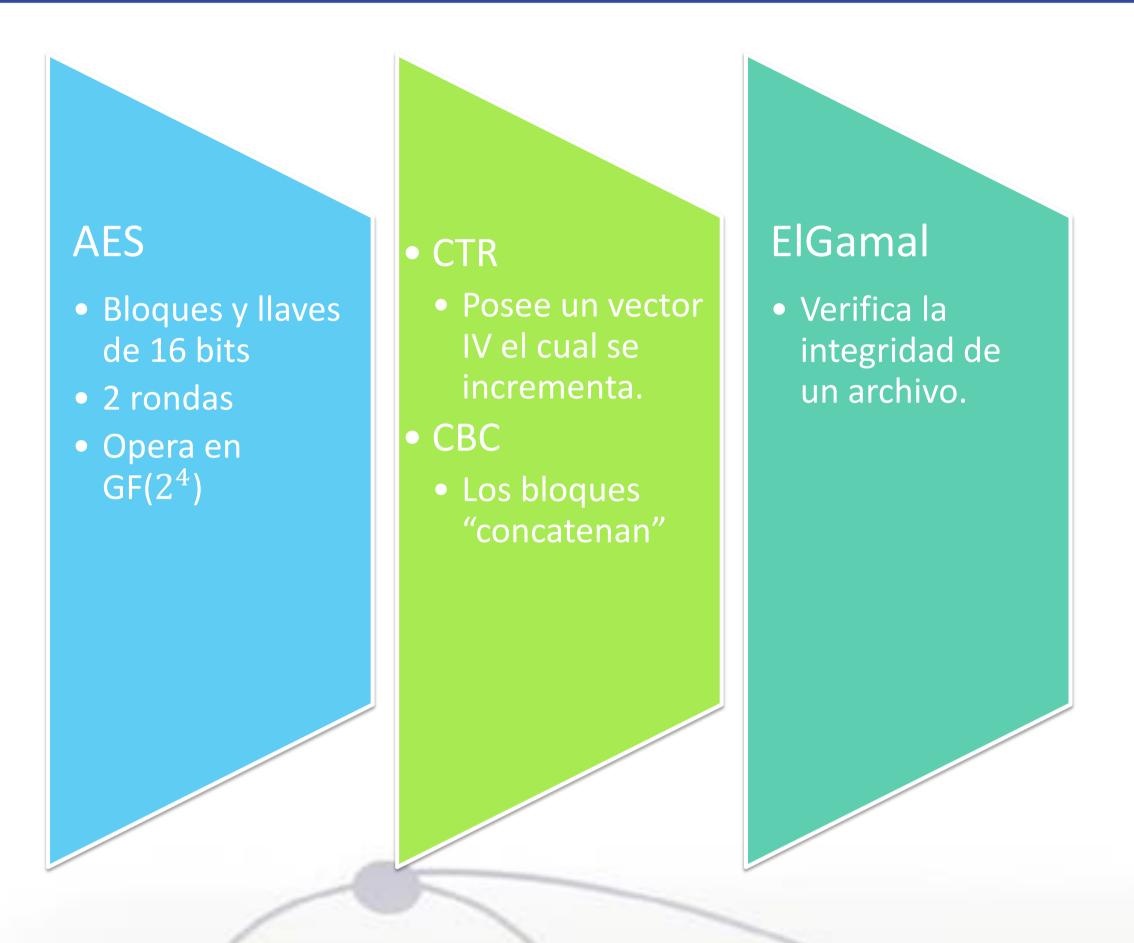
Hayde Barbosa – Alejandro Navarro

Cryptography 3CV2 – Escuela Superior de Computo ESCOM – IPN

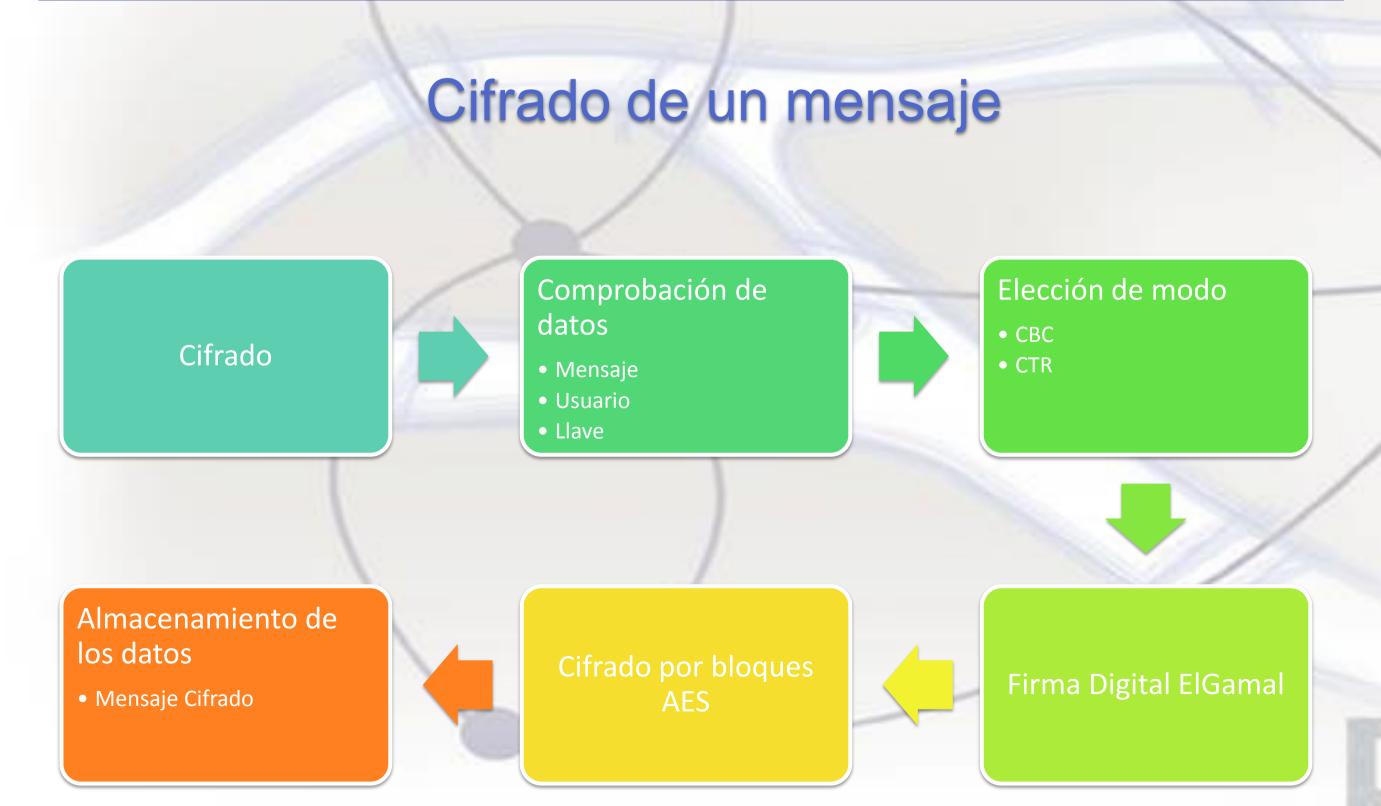
## Descripción de la aplicación

La aplicación se desarrollo usando el lenguaje de programación C. Se divide en varios "módulos" los cuales contienen las distintas funciones necesarias para el funcionamiento general de la aplicación.

## Características



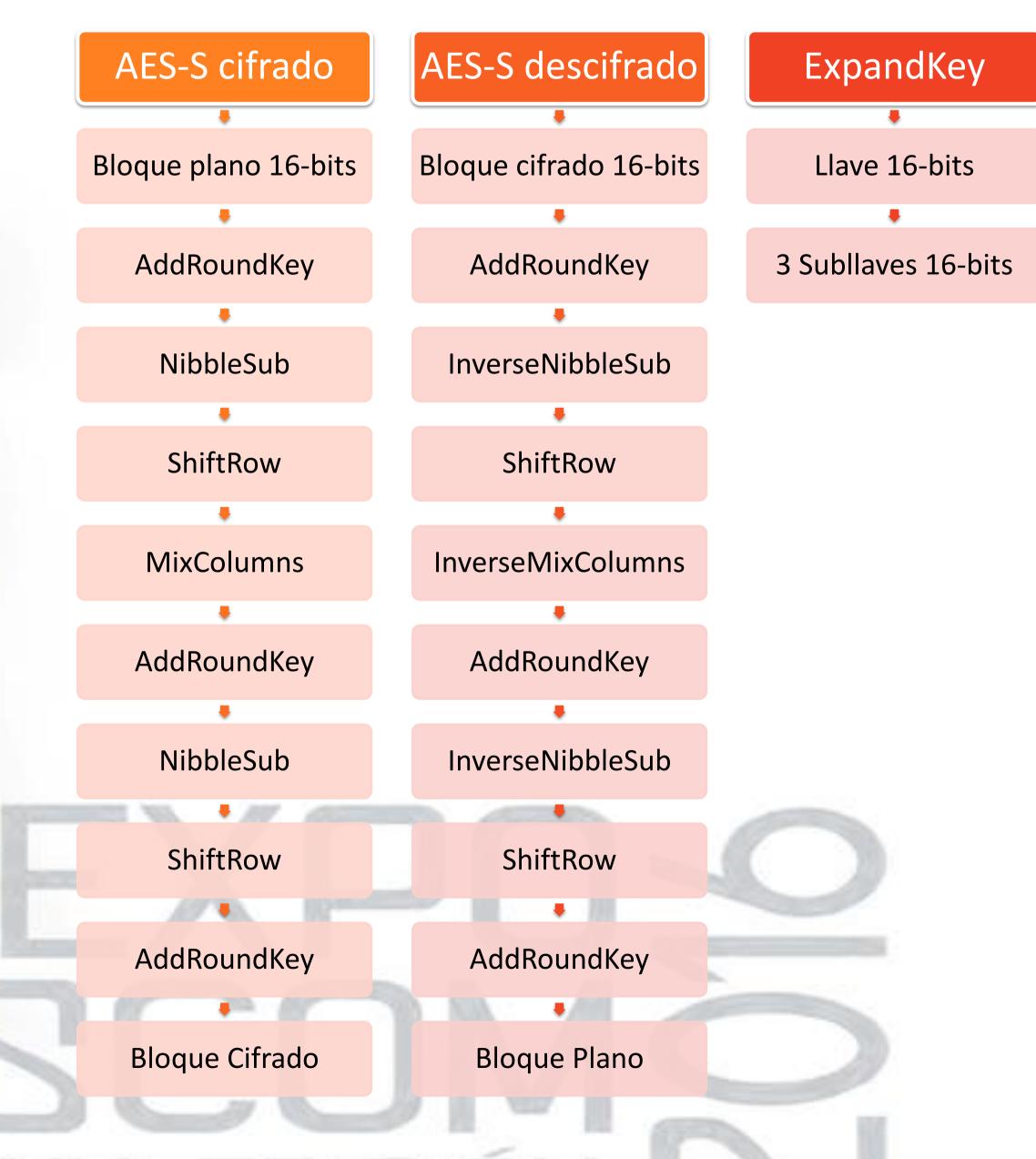
## Funcionamiento de la aplicacion



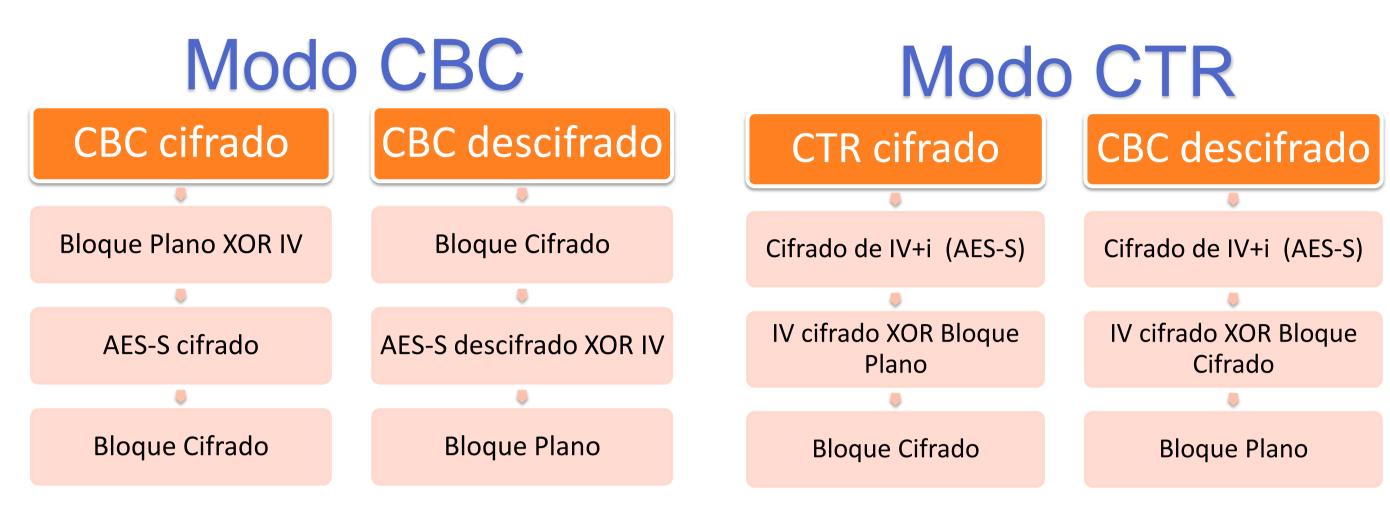
# Descifrado de un mensaje Comprobación de datos Mensaje Cifrado Mensaje Cifrado Modo Descifrado por bloques AES Almacenamiento de los datos Mensaje Mensaje Firma Digital ElGamal Comprobación de datos Comprobación de datos

## Algoritmos

## AES-S



### Algoritmos



- IV o bloque de inicialización: es un vector
  electorio.
  - i : 0 ≤ i ≤ numero de bloques 1

# Firma digital ElGamal

IV o bloque de inicialización: es un vector

