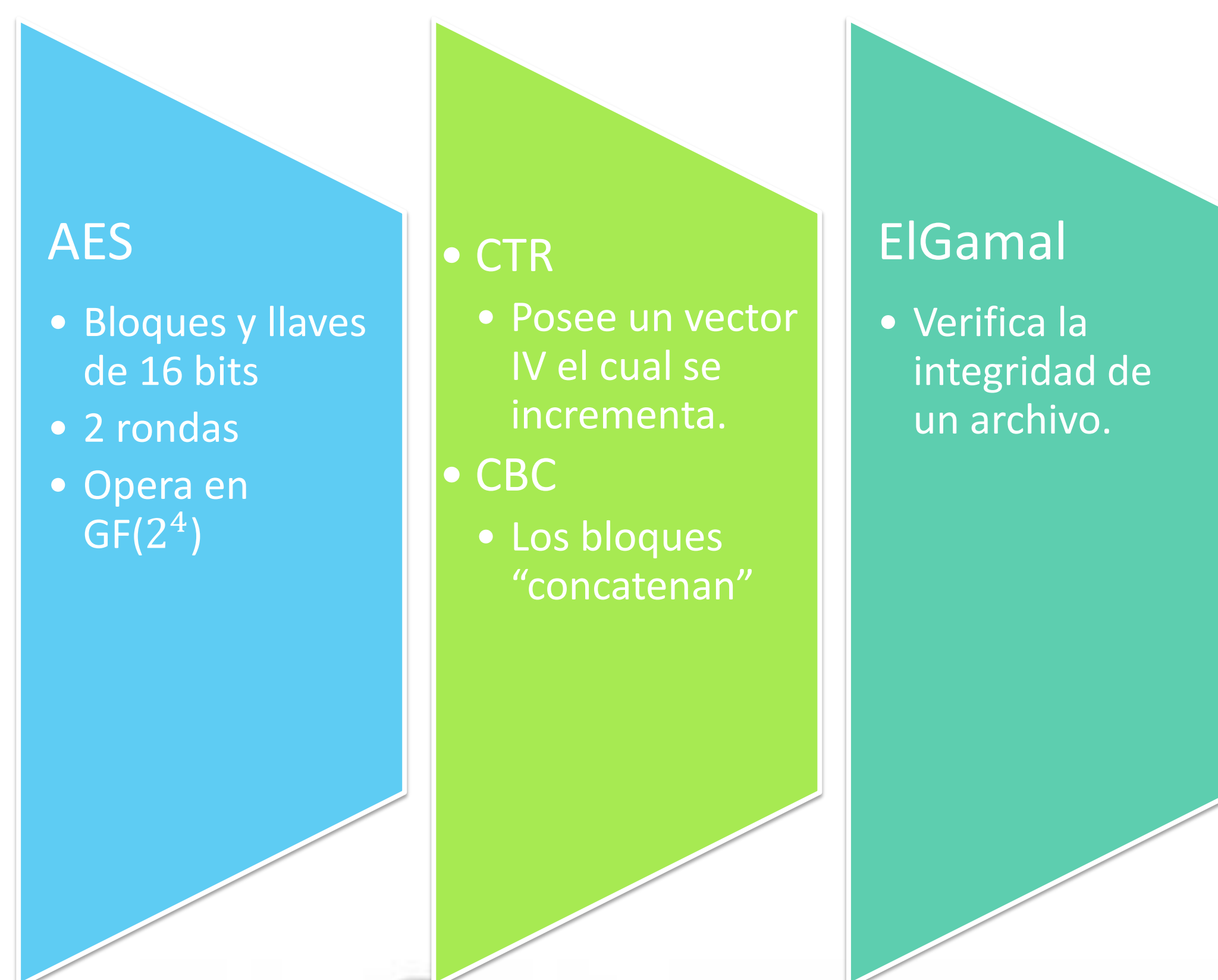


Descripción de la aplicación

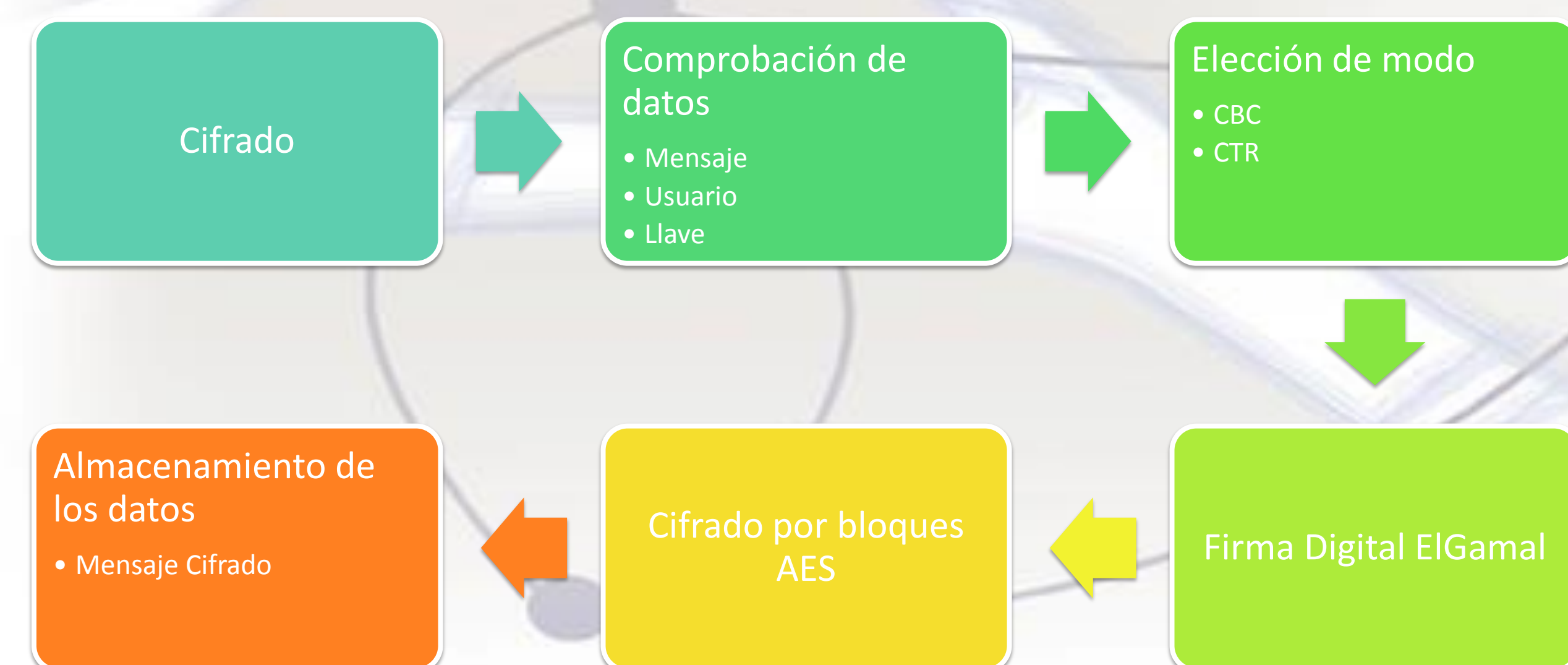
La aplicación se desarrollo usando el lenguaje de programación C. Se divide en varios "módulos" los cuales contienen las distintas funciones necesarias para el funcionamiento general de la aplicación.

Características



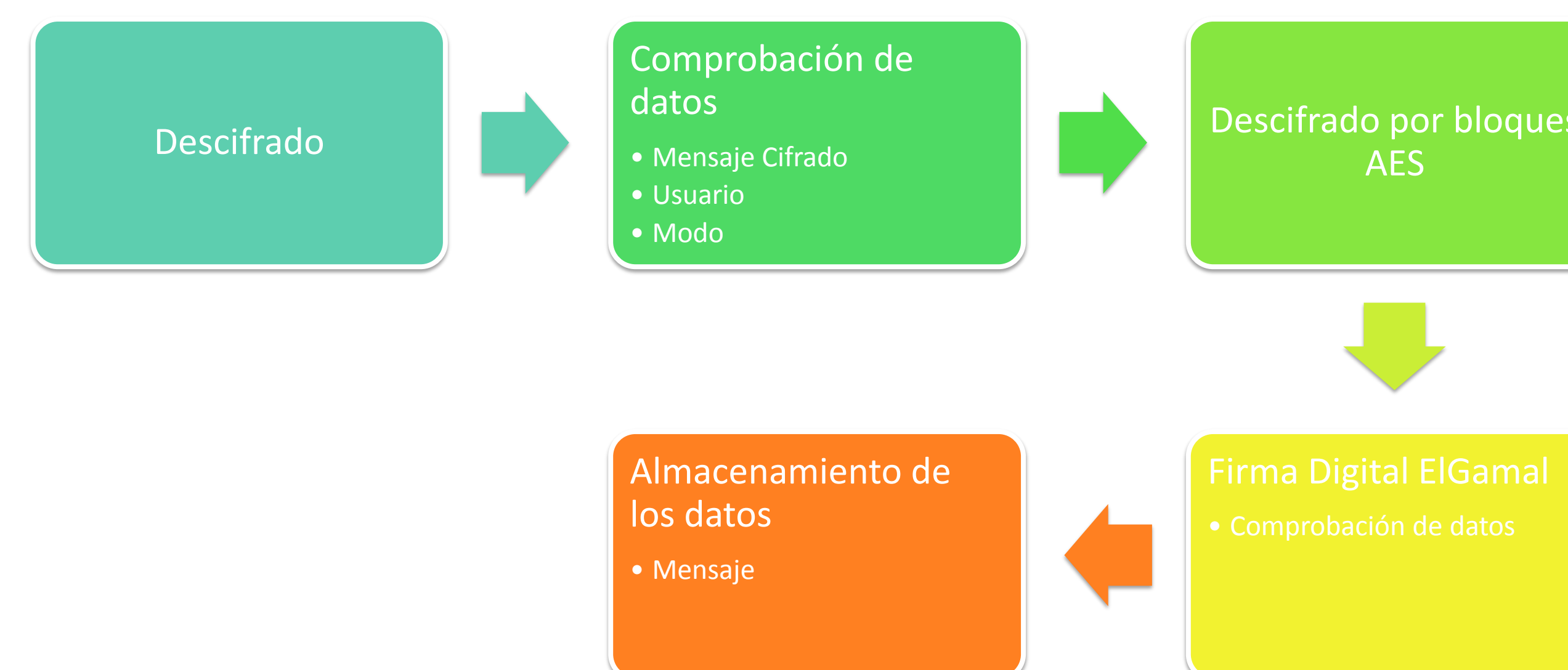
Funcionamiento de la aplicacion

Cifrado de un mensaje



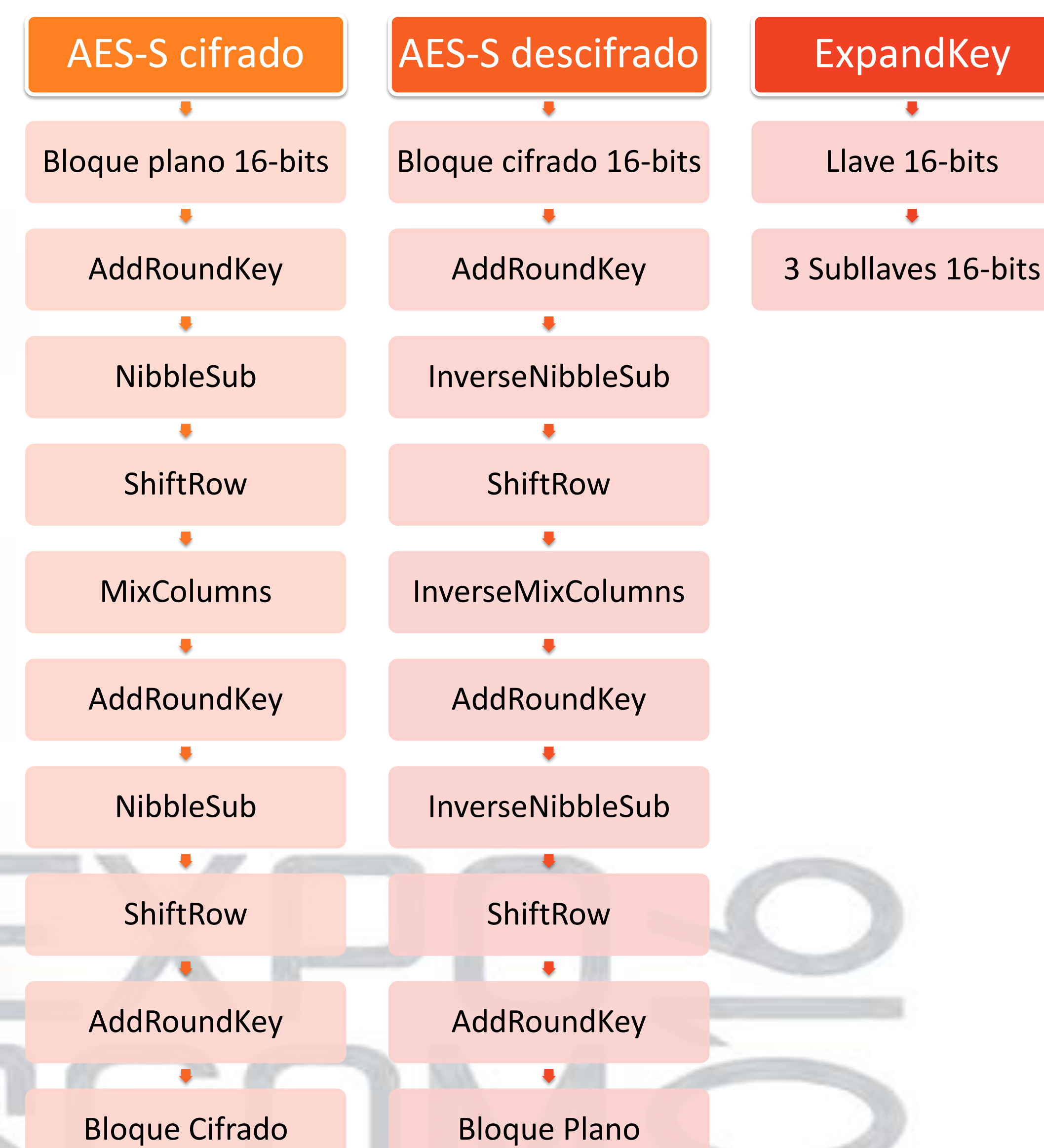
Funcionamiento de la aplicacion

Descifrado de un mensaje



Algoritmos

AES- S



Algoritmos

Modo CBC



- IV o bloque de inicialización: es un vector aleatorio

Modo CTR



- IV o bloque de inicialización: es un vector aleatorio
- $i: 0 \leq i \leq \text{numero de bloques} - 1$

Firma digital ElGamal

