Aes_Viewer

Implementation en c++ de l'algorithme de chiffrement AES

AES: Aes est un algorithme de chiffrement symetrique par blocs de 128 bytes

Install

- `git clone https://code.up8.edu/BrahimaDibassi/brick-destroyer.git`
- `make`
- `./Aes_img Images/blue_sky.jpeg`

Commande du viewer

Clique Droit -> Ouverture du menu

Menu :

Encrypt ECB -> Chiffrement via le mode Electronic Code Book.
Encrypt CBC -> Chiffrement via le mode Cipher Block Chaining.
Decrypt -> Dechiffrement de l'image

Explications

Ce Projet ce decoupe en deux module AES et Img_Viewer
Le Code source de AES : `Lib/aes.hpp et Lib/aes.cpp`
Le Code de l'image Viewer : `./Aes_img.cpp + Lib/stb_image.h`

Viewer

Basée sur le Menu utilisé en cours de Algorithmique Avancé.
Utilisation de la library STB pour la lecture d'image

AES

Documments : AES_SYNT , Reference Doc
Block Size = 128 bits
Key Size = 128 bits

Todo List

AES 128 Functions :

Enc_Dec :

- ☑ KeyExpension
- ☑ AddRoundKey

Encrypt :

- ☑ Sub_Block
- ☑ MixColumns
- ☑ ShiftRows

Decrypt :

- ☑ UnSub_Block
- ☑ UnMixColumns
- ☑ UnShiftRows

Dibassi Brahima
L3 Informatique