README
Projet AES en VHDL

Votre Nom

11 mai 2025

Description du projet

Ce projet implémente l'algorithme de chiffrement symétrique AES-128 (Advanced Encryption Standard) en VHDL. Il est destiné à être simulé et synthétisé pour une cible FPGA ou testé sous environnement GHDL.

Fonctionnalités

- Chiffrement AES-128 complet.
- Architecture modulaire (SubBytes, ShiftRows, MixColumns, AddRoundKey).
- Machine à états pour le contrôle du chiffrement.
- Testbench complet pour la validation.

Structure du répertoire

- `src/` : fichiers VHDL de l'implémentation.
- `tb/` : fichiers VHDL pour les testbenchs.
- `doc/` : documentation du projet.
- `sim/` : fichiers de simulation.

Utilisation

Simulation avec GHDL

```
# Compilation
ghdl -a src/*.vhd tb/tb_aes.vhd

#   laboration
ghdl -e tb_aes

# Simulation
ghdl -r tb_aes --vcd=sim/aes.vcd
```

Affichage de l'onde avec GTKWave

```
gtkwave sim/aes.vcd
```

Exemple de test

Le testbench fournit une clé et un bloc de texte clair, puis vérifie que la sortie correspond au texte chiffré attendu.

À faire

— Implémentation du déchiffrement AES.
— Optimisations de la surface logique.
— Intégration dans un système embarqué.

Licence

Ce projet est sous licence MIT. Voir `LICENSE` pour plus de détails.

Contact

Pour toute question, merci de contacter : `votre.email@example.com`