Université de Limoges

Développement Logiciel Cryptographique

TP n° 1 : Cryptanalyse SQUARE de l'AES

1 Cryptanalyse SQUARE de l'AES à 4 tours

- Implémentez en langage C la cryptanalyse SQUARE sur l'AES à 4 tours.
- Retrouvez la clé secrète correspondant aux λ-sets fournis.

2 Cryptanalyse SQUARE de l'AES à 5 tours

- Implémentez en langage C la cryptanalyse SQUARE sur l'AES à 5 tours.
- Retrouvez la clé secrète correspondant aux λ-sets fournis.