Mathieu Grandmontagne & Maël Nogues

TP Implémentation du Cipher Midori64

Le cipher Midori fait partie de la famille des Lightweight ciphers. Il s'agit d'une famille de cipher dont le but est d'obtenir une sécurité pertinente tout en utilisant le moins de puissance de calcul possible. Ce dernier point permet une consommation d'énergie minimale grâce aux calculs de l'algorithme, simple à exécuter pour les circuits électroniques.
Dans le cas du cipher Midori, l'implémentation peut se faire avec seulement des XOR et des décalages ce qui demande, d'un point de vue énergétique, moins de ressources qu'une multiplication ou d'autres opérations comme on peut trouver dans le cipher AES. C'est pour cela qu'on peut le qualifier de cipher écologique.

Commande pour compiler le programme :

```
$ gcc -O3 midori64 midori64.c
```