Programmation cartes à puces

Loïc Demange
loic.demange@etud.univ-paris8.fr

avec les notes de cours de Philippe Guillot

21/1 avril 2021

Attaques temporelles

En cryptanalyse, l'attaque temporelle consiste à analyser le temps d'exécution d'une opération pour en déduire des informations sur le secret.

Pour que ce genre d'attaque soit possible, il faut que le temps d'exécution soit lié au secret.

Attaques temporelles

Dans le projet carte SIM, le code PIN et le code PUK sont des secrets.

- Comment la vérification du code PIN/PUK peut faire fuiter de l'information ?

Projet carte SIM

Corriger la comparaison des codes PIN et PUK pour qu'elle soit "temps constant".