Introduction

Craquage de mots de passe

- Qu'est-ce que la **force** d'un mot de passe?
- Qu'est-ce qu'une fonction de **hachage cryptographique**?
- Pourquoi on **hache** les mots de passe?
- Qu'est-ce que le **salage** de mot de passe? (À quoi ça sert)

Fonctions de hachage

Exemples de hash de mots de passe

- md5("12345") = `827ccb0eea8a706c4c34a16891f84e7b`
- md5(“12346”) = `a3590023df66ac92ae35e3316026d17d`
- Une petite modification dans l’entrée produit un hash complètement différent
- MD5 est insécure car trop rapide à calculer
- Un outil comme John the Ripper casse ces hash en quelques secondes sur un laptop
- Encore plus rapidement avec une carte graphique (GPU) et un outil comme Hashcat