HEIG-VD — PCO

Laboratoire 2 – Rapport

[redacted]

28 octobre 2023

1 Description des fonctionnalités du logiciel

Les fonctionnalités de bases sont conservées, le logiciel permet de cracker des hashs de type MD5 par le moyen de force brute sur l'alphabet donné.

2 Choix d'implémentation

Nous avons décidé de séparer le traitement de manière égale entre tous les threads. Chaque thread traite une plage de possibilités pour la chaine finale.

Chaque thread va itérer sur sa plage de mots de passes potentiels jusqu'à ce qu'un d'entre eux tombe sur la bonne combinaison.

Quand la combinaison correcte est trouvée, le mot de passe est inscrit dans le pointeur référençant le `QString` de résultat donné à tous les threads. Le résultat étant unique, il n'y aura qu'un thread qui modifiera cette variable, évitant donc de devoir mettre en place une exclusion mutuelle.

Chaque thread vérifie avant d'effectuer une nouvelle itération que le `QString` donné par pointeur soit vide. S'il ne l'est plus (un autre thread a trouvé la solution), alors le thread arrête le traitement.

3 Tests effectués

Nous avons comparé le temps d'exécution pour une chaîne de caractères demandant une itération quasiment-complète `$z*9`. Pour un thread le temps étant d'environ 12 secondes, et le temps était réduit à environ 2 secondes pour 8 threads. Cependant, utiliser plus de threads n'améliore pas particulièrement les performances, les dégradant même après un certain nombre.

Nous avons aussi expérimenté avec une chaine de caractères plus longue, mais le temps nécessaire étant exponentiel, nous nous sommes limités à cinq caractères, comme conseillé pour ce laboratoire.

Nous avons également testé des cas qui pourraient sembler critiques, à savoir le premier mot de passe de certains threads. En effet, si ceux-ci échouaient, cela aurait montré un problème dans l'attribution de ces mots de passe initiaux, ce qui n'a pas été le cas chez nous.