HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Prof. Yann Thoma
Gregory Medwed
Fiorenzo Gamba

Laboratoire de Programmation Concurrente
semestre printemps 2020

Cracking md5

Temps à disposition : 4 périodes

1 Objectifs pédagogiques

— Se familiariser avec la gestion des threads
— Stopper élégamment des threads.

2 Récupération des sources

La récupération du code source s'effectue à l'aide d'un `git pull` dans le dossier du labo.

3 Cahier des charges

Nous sommes intéressés à développer un programme capable de cracker un hash md5 pour récupérer un mot de passe. Une application vous est gracieusement fournie, mais souffre de quelques carences en termes de performances. En effet, elle n'est pas multi-threadée pour les calculs à faire.

Le code correspondant au coeur de calcul se trouve dans la classe `ThreadManager`, dans la fonction `startHacking` pour le moment. A vous de modifier ce code de manière à lancer le nombre de threads demandé, d'attendre le résultat et de retourner le mot de passe trouvé. Vos modifications devront être réalisées à l'aide de la librairie `PcoSynchro` avec des threads `PcoThread`. Essayez d'avoir une solution la plus rapide possible. Il n'est par exemple pas nécessaire de laisser tourner tous les threads de calcul si l'un d'eux a trouvé la réponse.

La barre de progression est contrôlée par la fonction

```
void ThreadManager::incrementPercentComputed(double percentComputed)
```

A vous de faire en sorte de pouvoir utiliser cette fonction depuis vos threads afin d'avoir une progression pertinente.

Pour faire vos tests, le site web suivant vous permet de générer des hash md5 :

`https://emn178.github.io/online-tools/md5.html`

Si vous voulez utiliser un sel, alors le sel devra être placé avant le mot de passe sur ce site web. Par exemple, si votre sel est *xy* et votre mot de passe *mute*, alors placez *xymute* dans la saisie web.

4 Travail à rendre

— Ne pas créer de nouveau fichier. Modifiez et utilisez judicieusement les fichiers `mythread.h` et `mythread.cpp`, ainsi que la fonction `startHacking()`.

— Les modalités du rendu se trouvent dans les consignes qui vous ont été distribuées.

— La description de l'implémentation, ses différentes étapes, la manière dont vous avez vérifié son fonctionnement et toute autre information pertinente doivent figurer dans le fichier `rapport.pdf` fourni.

— Inspirez-vous du barème de correction pour savoir là où il faut mettre votre effort.

— Vous devez travailler en équipe de deux personnes.

5 Barème de correction

Conception	30%
Exécution et fonctionnement	20%
Codage	15%
Documentation et analyse	25%
Commentaires au niveau du code	5%
Robustesse	5%