

TRAVAIL PRATIQUE #1
GESTIONNAIRE DE FICHIERS CHIFFRÉS

Hiver 2026

Sécurité des Applications
(8INF333)

Groupe 01

Local : P3-1020

Département d'Informatique et de Mathématiques (DIM)

Florentin Thullier

Courriel : fthullie@uqac.ca

Bureau : P3-5040

Question Bonus (2 pts)

Répondez à la question suivante sans utiliser d'outils d'intelligence artificielle générative en une dizaine de lignes maximum. Le moindre doute quant à la génération de votre réponse par un LLM vous fera perdre vos points bonus potentiels.

L'application de gestion de fichiers chiffrés fournie pour ce premier travail pratique délègue les opérations cryptographiques à un processus séparé (processus enfant) plutôt que de les exécuter directement dans le processus principal qui est responsable de l'interface. Expliquez les motivations derrière ce choix.

Insérez votre réponse ici et n'oubliez pas de produire un fichier pdf et de supprimer le docx pour le rendu.

Il y a plusieurs raisons de choisir de mettre les opérations cryptographiques dans un processus enfant. Tout d'abord, il est plus facile de séparer la gestion d'interface de la gestion des calculs dans les programmes de manière générale. Ainsi, si présentement le processus cryptographique échoue, l'interface ne sera pas réellement affectée par l'échec. Ensuite, séparer le processus cryptographique de l'interface permet de garder les opérations sensibles dans son propre thread, cela réduit les angles d'attaque. Si une faille est trouvée dans le code de l'interface, elle ne peut pas être utilisée pour compromettre la cryptographie car le processus cryptographique est au final toujours seulement accessible par les entrées et sorties prévues.