Enoncé TP

A rendre par email avant le 21.01.2021à 23h59
niklaus.eggenberg@hesge.ch

En tant que cellule d'une organisation d'espionnage du gouvernement, vous avez intercepté un message codé via l'algorithme RSA. Ce message, qui vous a été fourni par voie séparée, contient le code secret pour protéger votre nation d'une menace imminente.

Votre mission, si vous l'acceptez, est de retrouver le message déchiffré, en utilisant les méthodes vues lors de votre formation d'agent secret. Vous devrez alors fournir un code et un rapport afin de convaincre vos supérieurs sceptiques qui n'y comprennent rien, que votre travail a permis de sauver la nation !

Ce message ne s'auto-détruira pas dans 15s. !

Rapport et rendu

1. Pensez à donner le nom complet de chaque membre du groupe en première page,

2. Ecrivez une brève introduction sur le contexte du TP. Soyez créatifs pour mentionner les fondements théoriques du cours sans pour autant copier les slides !

3. Décrivez COMMENT vous avez implémenté les méthodes – sans pour autant fournir votre code ni une documentation de ce dernier.
   Le but est de décrire les astuces d'implémentation non triviales. Donnez au moins le nom des méthodes implémentées (dans la théorie, pas dans le code !), ainsi que les astuces d'implémentation (exemple typique : le pgcd assume que le premier nombre est le plus grand…).

4. Présentez vos résultats ainsi qu'une analyse de la performance (basée sur des mesures et/ou des approximations pour les très grands nombres, comme vu au cours).

5. Pensez à TOUJOURS justifier vos propos. Evitez les « on sait que », « on montre que » ou les conclusions non-justifiées du type « A est plus complexe que B ». Posez-vous toujours la question « pourquoi est-ce le cas » et, si la réponse n'est pas triviale, expliquez (parfois, 3 mots suffisent !).

6. Pour la structure, il vous faudrait une introduction, une motivation théorique, une partie méthodologique, la présentation des résultats ainsi qu'une conclusion.

7. Le rendu du tp se fait sous forme électronique : le rapport sous forme PDF, le code-source sous forme d'archive (.zip ou autre).