

Enoncé TP

A rendre par email avant le 21.01.2021 à 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-détruit 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 ! Rappelez-vous que vous devez convaincre vos supérieurs que votre méthode est la bonne, mais que, comme tout bon supérieur qui se doit, il ne comprendra pas les détails, mais aimera entendre le nom de vos informateurs et vos sources!
3. Sans pour autant fournir votre code ni une documentation de ce dernier (le boss n'est pas programmeur !), décrivez votre approche dans les grandes lignes. Privilégiez le « Pourquoi cela fonctionne » plutôt que le « comment l'avons-nous codé ». Mentionnez également les éventuelles astuces d'implémentation non triviales ou les bugs rencontrés, qui assureront aux prochains agents de ne pas reproduire les mêmes erreurs !
4. N'oubliez pas de présenter votre résultat final et convainquez vos dirigeants de votre performance hors normes. Expliquez pourquoi vous avez réussi à craquer un code que la théorie dit devoir prendre des milliards d'années !
5. Pensez à TOUJOURS justifier vos propos. Vos supérieurs sont très à cheval là-dessus. Evitez les « on sait que », « on montre que », les relatifs vagues du genre « très long » ou « trop long » ou encore les conclusions sans fondement 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, privilégiez le classique : une brève introduction contextuelle (le boss a plein de projets, il doit se rappeler de quoi parle le vôtre), une partie méthodologique (qui se base sur vos informateurs !), la présentation des résultats ainsi qu'une conclusion.
7. Votre rapport est attendu sous forme électronique : envoyez-le sous forme de PDF et joignez-y le code-source sous forme d'archive (.zip ou autre).