Présentations du TP

Après l'examen oral, envoyez un fichier zip contenant le code source et l'éventuel support de votre présentation via email à niklaus.eggenberg@hesge.ch

Points à considérer pour l'oral

- Prévoyez une présentation d'environ 15 minutes, pas plus (je couperai après 20 minutes !)
- Pensez à équilibrer le temps de parole entre les différents membres du groupe
- Faites une rapide mise en contexte (expliquez ce qu'il vous est demandé de faire)
- Sans pour autant redonner toute la théorie du cours dans les détails, évoquez les éléments que vous avez utilisé
  ATTENTION : pensez à expliquer à quoi correspondent les divers éléments ! Par exemple, évitez de dire « on trouve p et q ainsi ». Précisez ce que sont p et q !
- Expliquez les parties qu'il vous a fallu programmer sans pour autant présenter / commenter le code pendant la présentation. Ne mentionnez que les éventuelles astuces techniques, problèmes rencontrés ou autres notions qui vous semblent pertinentes ou mettre en valeur votre travail.
- Faites une petite démonstration de l'exécution du logiciel (si cela ne prend pas trop de temps – la sortie console suffit !)
- En vous basant sur vos observations pour craquer votre clé (ici, c'est une clé sur 32 bits), estimez le temps qu'il vous faudrait, avec votre code sur votre machine, pour craquer une clé en RSA-1024,
- Pensez à ajouter une conclusion à votre présentation

A la fin de la présentation, des questions vous seront adressées individuellement.

La note sera toutefois établie de manière unique pour tous les membres du groupe !

Le champ des questions possibles est restreint à la théorie liée au RSA, à savoir

- Arithmétique modulaire
- Exponentiation rapide
- Bachez-Bézout et Euclide étendu,
- Principe général du RSA.

A la fin de l'examen, il vous sera communiqué une fourchette pour votre note, qui sera confirmée après vérification (éventuelle) du code source !