Cryptographie, HE-Arc, Automne 2025

Travail pratique 2

- Soumettre les trois exercices suivants:
    1. a) Quel algorithme de chiffrement et quelle longueur de clé utilisez-vous pour accéder au serveur GitLab de la He-Arc? Justifiez votre réponse en joignant votre clé publique.

       b) Votre solution est-elle considérée comme sécure contre les attaques classiques? Si ce n'est pas le cas, régénérez vos clés et mettez à jour votre accès à GitLab.

       c) Votre solution est-elle considérée comme sécure advenant la disponibilité d'un ordinateur quantique? Justifiez votre réponse.
    2. Devoir 7, exercice 6 (hachage).
    3. Devoir 8, exercice 6 (Diffie-Hellman).
- À soumettre sur Cyberlearn au plus tard le **jeudi 8 janvier à 23h59**.
- Vous pouvez travailler seuls ou en équipes de deux ou trois. **Une soumission par équipe, mais pour l'exercice 1 vous devez inclure la solution de tous les membres de l'équipe.**
- Soumettre un fichier `.ipynb` contenant:
    - Les noms des équipiers.
    - Les réponses aux exercices.
    - Les explications et autres informations pertinentes.
    - La forge git permettant à l'enseignant de consulter le code source et les commit.
- **Si vous ne soumettez pas exactement un fichier `.ipynb` , j'applique une pénalité de 20%.**
- **Si je ne peux pas accéder à la forge git sans vous contacter, j'applique une pénalité de 20%.**
- **Si je ne peux pas exécuter votre code directement, j'applique une pénalité de 20%.**
- **Tout usage d'un LLM doit être scrupuleusement et précisément décrit.**