

Devoir I

Dû le mardi 29 septembre 2026

Instructions : Il y a dix problèmes. Chaque problème vaut dix points pour un total de cent points. Pour chacun des problèmes, présenter une solution détaillée et soignée qui soit lisible et compréhensible pour une personne ne connaissant pas a priori la solution. Chaque réponse doit être pleinement justifiée. Il est possible de travailler en équipe avec d'autres étudiants, mais ultimement, il est important que chacun écrive sa propre solution. Seulement les devoirs écrits à la main seront acceptés.

1. Sur l'une des étagères de votre bibliothèque de quartier se trouve une longue bandelette sur laquelle figure la suite de caractères suivante :

LAIM IANVIST TARO DOI.NMINT IS IJNPVPLAUAOA ZIRYSA TIL LM T ALAVIN URIOADMQNNROAUG :RR.AT

Donner un sens à ce cryptogramme en trouvant la scytale qui sied tout juste à cette bandelette.

2. Expliquer comment le système de codage faisant appel à des scytales peut être vu comme un cas particulier du chiffrement par permutation de blocs de m lettres décrit à la § 2.5 de [1].
3. Faire le numéro 2.1 des exercices du chapitre 2 des notes de cours [1]. La tabula recta de la page 5 des notes de cours pourrait être utile.
4. Décoder le cryptogramme

GDAGG FXAVA AAVAX AFDGV GXGXF
XGVAG GVXFA XGDDX XAADA DFVXA
FAXGX XAFAF GXAXA XFAXA FFXFV
GXXAD VFFGF VXGXG ADADD FGDXX

du système ADFGVX en utilisant la grille (7) des notes de cours [1] et la permutation

(5, 11, 20, 2, 7, 13, 10, 16, 1, 8, 15, 3, 6, 19, 14, 4, 18, 12, 17, 9).

5. Faire le numéro 2.3 des exercices du chapitre 2 des notes de cours [1].
6. Faire les sous-questions a et b du numéro 2.4 des exercices du chapitre 2 des notes de cours [1].

7. Faire le numéro 2.5 des exercices du chapitre 2 des notes de cours [1].
8. Faire le numéro 2.9 des exercices du chapitre 2 des notes de cours [1].
9. Faire le numéro 2.12 des exercices du chapitre 2 des notes de cours [1].
10. Faire le numéro 2.13 des exercices du chapitre 2 des notes de cours [1].

Références

- [1] François Bergeron et Alain Goupil. La cryptographie de l'antiquité à l'internet. disponible en ligne : <https://bergeron.math.uqam.ca/wp-content/uploads/2014/04/crypto.pdf>, 2014.