

INITIATION À LA CRYPTOGRAPHIE
Master 1 Informatique
TP 1 – Cryptographie classique - Vigenère

Fabien Teytaud

Chiffrement de Vigenère

Chiffrement

Ecrire l'algorithme de vigenère. Le choix du langage est laissé libre. La clé et le texte à chiffrer seront passés en paramètres.

Le résultat du chiffrement sera écrit dans un fichier *texteChiffre.txt*.

Déchiffrement

Ecrire l'algorithme permettant le déchiffrement. La clé et le texte à déchiffrer seront passés en paramètres.

Le résultat sera écrit dans un fichier *texteClair.txt*.

Vous pouvez utiliser les options `-c/-d` en paramètre de votre programme pour les chiffrements et déchiffrements.

Cryptanalyse de cet algorithme

Vous trouverez [ici](#) et [là](#) deux textes en anglais chiffrés avec Vigenère.

Vous devez vous débrouiller avec les outils vus en cours afin de retrouver les clés utilisées pour les deux chiffrements.

N'hésitez pas à me demander si vous avez des questions.

Bonne chance !