TP3 : Le chiffre de Vigenère

Dans ce TP, vous devez répondre aux questions posées en écrivant les fonctions demandées avec le bon prototype. Tout manquement à ces instructions entrainera une perte de points lors du rendu.

Dans ce TP, nous verrons comment fonctionne le chiffre de Vigenère.

1 Le TP2 : dernière chance pour le corriger et le compléter (45mn maximum)

Vous trouverez, sur Moodle, le résultat des évaluations automatiques du TP2, sur le décodage de Cesar. Si votre programme a été noté comme ayant des problèmes, vous pouvez le corriger dès à présent, et effectuer un nouveau dépôt de votre travail (ce sera le dernier concernant le TP1). N'oubliez pas de suivre à la lettre les instructions de rendu données dans le TP2. Vous devrez effectuer votre rendu avant 9h15.

2 Le chiffre de Vigenère (2h)

Le chiffre de Vigenère ressemble au code de César, si ce n'est que le décalage à effectuer n'est pas le même selon la position de la lettre dans le texte. Il a été utilisé pour la première fois pendant le 16° siècle, et resta pendant près de trois siècles invaincu. La méthode que nous allons étudierons plus tard pour le "casser" fut proposée au début du 20° siècle, et finit par enterrer définitivement l'utilisation de ce chiffrage.

Imaginons que l'on souhaite chiffrer la phrase "la programmation, c'est vraiment bien!" (juste les lettres, on ne touche pas aux signes de ponctuation). On choisit tout d'abord un mot de passe que le destinataire du message doit aussi connaître : par exemple, choisissons "java" comme mot de passe. Le mot de passe doit alors être transformé en une série de nombres, chacun correspondant à la position de la lettre dans l'alphabet : ici, "java" devient 10-1-22-1.

Pour chiffrer le message, on décalera la première lettre de 10 places, la seconde d'une place, la troisième de 22 places, la quatrième de 1 place, puis on boucle : la cinquième lettre sera décalée de 10 places, la sixième lettre sera décalée d'une place, etc...

Notre message devient alors :

```
l a    p r o g r a m m a t i o n  ,  c ' e s t   v r a i m e n t   b i e n  !
10 01  22 01 10 01 22 01 10 01 22 01 10 01 22    01   10 01 22   01 10 01 22 01 10 01 22   01 10 01 22
-------------------------------------------------------------------------------------------------------
 v b    l s y h n b w n w u s p j  ,  d ' o t p   w b b e n o o p   c s f j  !
```

On voit dans le résultat que deux lettres différentes à l'origine peuvent devenir la même lettre dans le message crypté, et deux lettres similaires dans le message original peuvent devenir différentes dans le message crypté.

> **Questions**
>
> Proposez un programme demandant à l'utilisateur de saisir un nom de fichier contenant un texte, puis un mot de passe, et réalise le chiffrage de ce texte selon la méthode de Vigenère. Lisez bien la section suivante qui détaille le format de rendu de votre travail. Les lettres accentuées doivent, tout comme les chiffres et les signes de ponctuation, être ignorées.

3 Rendu du codage de Vigenère

Vous devez rendre le travail réalisé pour le TP3 sur Moodle ou par mail, à l'adresse

si vous n'avez pas de compte Moodle (et seulement à cette condition).

Ce rendu doit suivre un format spécifique. Votre programme devra s'exécuter à l'aide de la commande

```
./vigenere_codage mon_message.txt mon_mot_de_passe sortie.txt
```

où *mon_message.txt* est le message à coder, *mon_mot_de_passe* est un mot de passe uniquement constitué de lettres minuscules, et *sortie.txt* contient le message chiffré par la méthode de Vigenère. De plus, votre programme devra compiler à l'aide de la commande

```
gcc vigenere_codage.c -o vigenere_codage
```

Si votre ligne de compilation est plus complexe, vous devrez alors la spécifier dans un *Makefile*. Tous vos fichiers devront être directement placés dans un fichier zip (et ne pas être dans un sous dossier du fichier zip), dont le nom sera

```
VotreNom_VotrePrenom_VotreNumeroEtudiant.zip
```

sans aucun espace (si votre nom ou votre prénom contiennent un espace, ne les faîtes pas figurer). Les formats de compression acceptés sont .zip, .tgz, .tar.gz, .7z, .rar.

Si vous avez un binôme, il vous faudra écrire son nom, prénom et numéro d'étudiant séparés par des espaces, en plus des vôtres, dans un fichier *binome.txt*, dont le format sera

```
Nom1 Prenom1 Numero_etudiant1
Nom2 Prenom2 Numero_etudiant2
```

Vous ne devez rendre le fichier qu'une seule fois par binôme.