Chiffrement et encodage

Ce TD est inspiré de l'épreuve 2008 d'informatique du concours de l'X en MP option SI.

Le but de ce TD sera de crypter un message en utilisant deux types de codages "simple": Codage César et Codage Vigenère.

1 Chiffrer un message

Avant de crypter le message il faut le rendre manipulable par l'outil informatique. Un message `M` (une liste de lettres - on oubliera les espaces et les signes de ponctuations) doit donc être tranformé en une liste de nombres `L` ($a \leftrightarrow 1$, $b \leftrightarrow 2$..).

Exemple sur `jaimelesmahts`:

liste `M`	j	a	i	m	e	l	e	s	m	a	t	h	s
liste `L`	10	1	9	13	5	12	5	19	13	1	20	8	19

- Écrire une procédure `Chiffre` qui chiffre un message.
- Écrire une procédure `Dechiffre` qui déchriffre un message.

2 Codage de César

Le codage César consiste à décaler l'alphabet d'un nombre donnée `d`, la clé. Ainsi pour `d` = 1, `jaimelesmaths` devient `kbjnfmftnbxgt`.

- Écrire une procédure `CodeCesar` prenant en argument `M` le message et `d` la clé et renvoyant `M'` le message codé.
- Écrire une procédure `DeCodeCesarCle` prenant en argument `M'` le message codé et `d` la clé et renvoyant `M'` le message.

3 Casser le codage César

Pour casser le codage César, il faut découvrir `d`, la clé. On pourrai essayer tous les décalages possibles et voir lequel donne un texte cohérent mais ce serai pénible. Une autre solution consiste à calculer la fréquence d'apparition de chaque lettre. En effet, l'étude de la langue français indique que sur des textes suffisamment long, la lettre la plus courante est le `e`. Ainsi si notre message est suffisamment long, la lettre la plus fréquente correspondra à `e` et on pourra calculer le décalage.

- Écrire une procédure `Frequence` qui prend en argument le message `M` et qui renvoie la lettre la plus fréquence.
- Écrire une procédure `DecodeCesarAuto` qui prend en argument le message `M'` et qui renvoie le message décrypté `M`.

4 Codage de Vigenère

Au XVIe siècle, Blaise de Vigenère a modernisé le codage César. Au lieu de décaler toutes les lettres du texte de la même manière, on les décale en fonction d'une clé. Prenons la clé `nimajneb`. Ainsi on codera la première lettre en utilisant le décalage qui envoie `a` sur `n` (c'est à dire de 13), la deuxième lettre du décalage qui envoie `a` sur `i` et ainsi de suite. Quand on arrive à la fin de la clé, on recommence par le début.

- Écrire une procédure `Vigenère` qui prend en argument le message et la clé et qui renvoie le message crypté.
- Écrire une procédure `DecVigene` qui décode un message crypté en connaissant la clé.

Pour casser le codage de Vigenère, vous pouvez regarder la fin de l'épreuve de l'X.