Partie 1

Chiffrements symétriques

1.1 Vocabulaire

- **Chiffrer** : transformer les caractères d'un texte pour le rendre incompréhensible, sauf pour celui qui possède la clé de chiffrement.
- **Déchiffrer** : transformer le texte chiffré en texte clair à l'aide de la clé de chiffrement
- **Décrypter** : transformer le texte chiffré en texte clair sans posséder la clé.
- **Cryptologie** : science du secret : possède deux branches
  - **cryptographie** : étude de l'art du chiffrement
  - **cryptanalyse** : analyse des méthodes de chiffrement pour les casser (décrypter)

1.2 à quoi sert le chiffrement ?

Le chiffrement a pour but de protéger nos données, nos communications, mais aussi de signer nos messages et de s'assurer que l'on communique bien avec la bonne personne :

- **Authentification** : L'authentification est la procédure qui consiste, pour un dure qui consiste, pour un système informatique, me informatique, à vérifier l'identit rifier l'identité d'une d'une entité (personne, programme, machine).
- **L'intégrité** des données désigne le fait que les données ne soient pas modifiées au cours d'une communication ou de leur stockage. Ainsi, si vous envoyez un texte chiffré sur un canal non sécurisé, le texte chiffré pourra être intercepté et altéré par un attaquant avant d'atteindre son destinataire. Pour contrôler cette intégrité, on associe au message une valeur de contrôle.
- **La confidentialité** : Le chiffrement permet de protéger la confidentialité de vos données à l'aide d'une clé secrète.

1.3 Chiffrement par substitution monoalphabetique

Pour ce type de chiffrement, chaque lettre de l'alphabet est transformée en une nouvelle lettre. Et cette nouvelle lettre est unique.

Ici, la fonction utilisée pour le chiffrement de César, est un simple décalage :

$$x \to x + cle$$

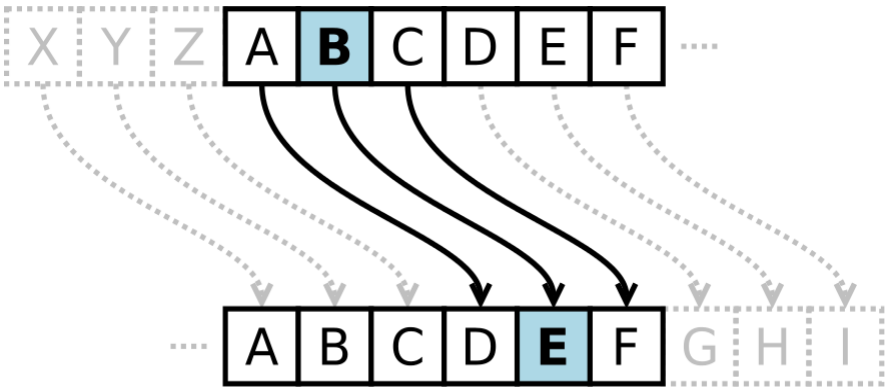

FIGURE 1 – Chiffrement par décalage - wikipedia

Cet algorithme de chiffrement utilise une fonction périodique pour transformer les rangs de chaque lettre :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Compléter l'algorithme du chiffrement de César. On suppose qu'il existe une clé `c` correspondant au décalage utilisé. Le message clair est `m` et le message chiffré est `m_chiffre`

```
Pour chaque lettre l du message m:
  l_chiffre = ...
  m_chiffre = ...
```

Combien faudra-t-il faire d'essais, au maximum, pour decrypter ce message par une méthode dite de force brute ? N < ….

Expliquer pourquoi ce type de chiffrement peut-être facilement decrypté par analyse frequentielle ?

1.3.1 Substitution polyalphabétique

Polyalphabetique : Se dit d'un chiffre où un groupe de n lettres est codé par un groupe de n symboles.

- L'exemple suivant montre une polysubstitution simple avec une clé de longueur 3 qui va décaler les lettres de l'alphabet :

On définit la clé '123' qui indique que le premier caractère sera décalé d'une position, le second de 2 et le troisième de 3 positions, etc.

Le mot : WIKIPEDIA donne donc dans ce cas XKNJRHEKD.

- La machine Enigma utilisait ce principe de codage, à l'aide de 3 rotors.
- Le chiffrement *Playfair*, (voir le cours en ligne) s'apparente à une substitution polyalphabetique, puisqu'il substitue des digrammes (groupes de 2 lettres) dans le texte d'origine.

1.3.2 Points communs des chiffrements symétriques

Ces algorithmes fonctionnent selon :

- Entrée
- repetition n fois de substitutions et permutations. Utilise une clé unique pour chiffrer et dechiffrer.
- Sortie

Pour le chiffrement symétrique, le seul secret, c'est la clé de chiffrement.

Partie 2

Exercices

2.1 Substitution monoalphabétique : Code de César

2.1.1 Quelle clé a été utilisée pour chiffer ce texte (avec l'algorithme de César) ?

jyfwavnyhwopl hwwspxbll

2.1.2 Décrypter ce message.

2.1.3 Proposer un programme en python qui chiffre un message clair `m` en un message codé selon la clé numérique `c`.

Aide :

- La fonction `ord('x')` retourne un entier correspondant à la position d'un caractère dans la table ascii. Par exemple, `ord('A')` retourne 65, `ord('B')` retourne 66,...
- La fonction `chr(N)` retourne le caractère de rang N : `chr(65)` retourne 'A'.

2.2 Substitution polyalphabétique : Chiffrement de Playfair

A partir des explications données dans la video :

2.2.1 Construisez la matrice pour l'algorithme de Playfair avec la clé *estienne*.

2.2.2 Chiffrer le message : *COUPERLETRANSMETTEUR*.

2.2.3 S'agit-il d'une méthode utilisant la substitution monoalphabetique, ou polyalphabetique ?

2.2.4 Est-ce qu'avec cette méthode, le decryptage peut être facilité par l'analyse fréquentielle ?

2.3 Frequences des lettres dans un texte

La fonction suivante retourne une liste de 26 valeurs de type *float*, donnant dans l'ordre de l'alphabet, la frequence pour chaque lettre dans un texte :

```
def freq(m):
    frequences = [0]*26
    n = len(m)
    for c in m:
    ...
```

Compléter le script de la fonction `freq`.