Exercice 1

Etape 1 : chiffrement à decalage

D'après le cours on sait que le chiffrement par decalage la clé est $K = (1, b)$

Pour dechiffrer la formule est

$$d_K(y) = a^{-1}(y - b) \bmod m$$

Il faudrait on le brute en utilisant la force brut (recherche exhaustive) en essayant tous les couple $(1, b)$ qui donne un sens au message

Je vais elaboren mon code de la manière suivante:
Je vais donc prendre mon message chiffré, et determiner d'abord pour chaque lettre sa correspondance en nombre ensuite je vais appliquer ma formule pour chaque lettre dans le message chiffré, c'est à dire $(y-b) \bmod 26$ je ne rajoute pas le a dans la formule, car $a^{-1} = 1^{-1} = 1$ dans $\mathbb{Z}/26$ j'ai utiliser pow(1,-1,26) pour savoir il faut noter que b, a & 6 valeurs possibles dans notre cas on va essayer, chacun et trouver le message qui fait du sens.
Note: Mon code sera en Python

Après l'execution de mon code :
J'ai d'abord copié le message comme dans l'enoncé et j'ai rien remarqué de particulier mais après avoir retiré les espaces j'ai remarqué quelque chose interessant pour le decalage

La chiffre recherché est 3

Etape 2 : chiffrement affine

Pour le chiffrement affine je vais proceder de la même maniere que l'etape1 mais

mais dans ce cas le pgcd(a,m)=1
Dans notre cas pgcd(a,26)=1

Pour les valeurs possibles de a
on a 12 car phi(26)=12

les valeurs possible de b reste
inchangé càd 26 on va passer
par la force brute et tester les
combinaison (a,b) et trouver
celui qui fais du sens le code
sera structuré de la même
manière que Etape 1 sauf
que on va rajoute a cette
fois ci

Après l'execution j'ai trouvé quelque chose intennessant pour
a = 25 et b = 16
on demande combien il y'a Etapes dans ce exercices ?
le deuxieme code est 5

Etape 3 : CHIFFREMENT DE HILL

Jamais deux sans Trois

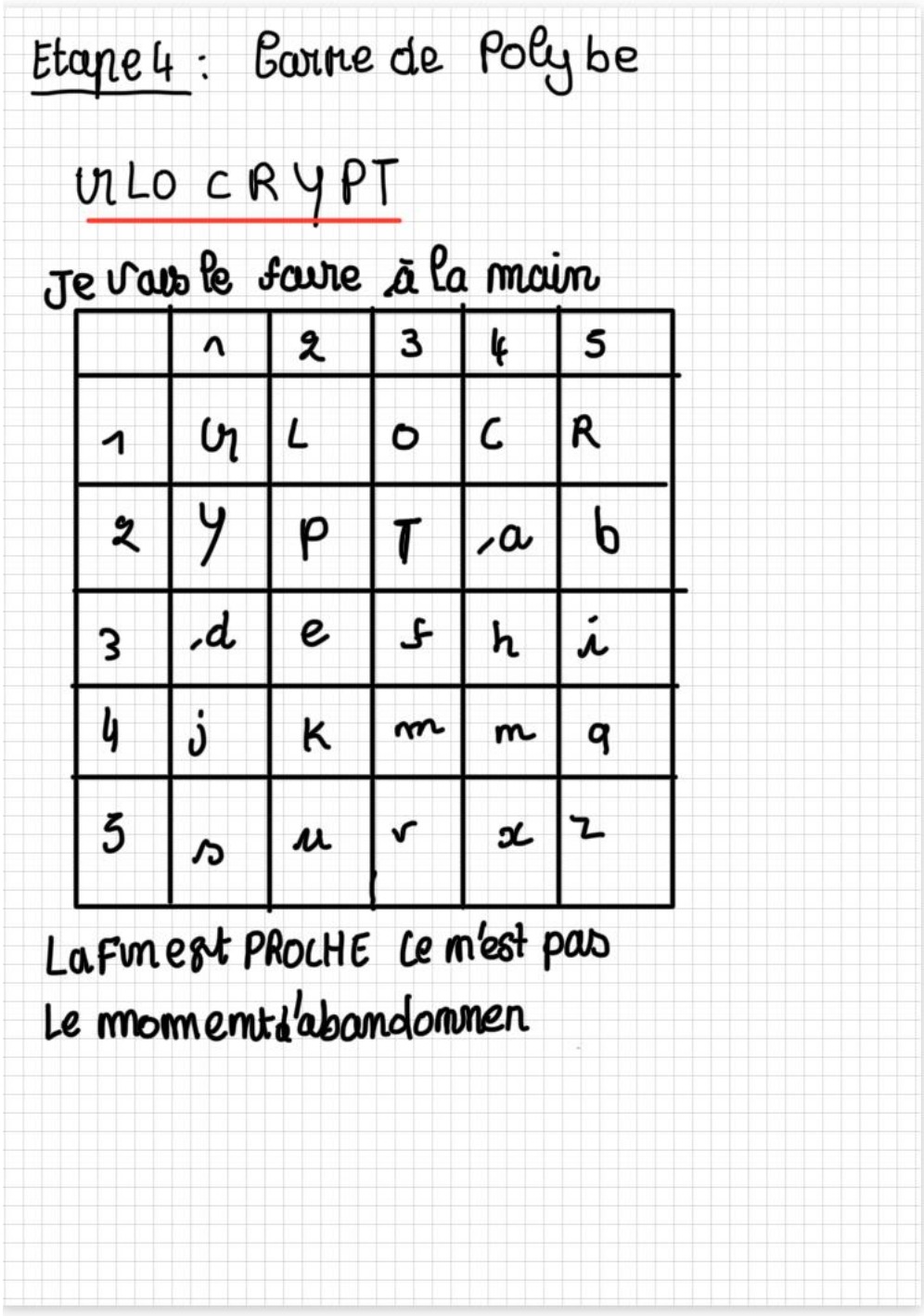
HaHax

J'ai coder le HILL, en utilisant le système 1 et 2 et j'ai fini Par conclure d'après l'indice que la version chiffrer est

BCKUSYZEWHCEHCV

JWEEZCVOR

la code est ZEWH qui correspond à 2



	1	2	3	4	5
1	U	L	O	C	R
2	Y	P	T	a	b
3	d	e	f	h	i
4	j	K	m	m	q
5	s	u	v	x	z

J'ai obtenu le résultat suivant :
122433354432512322151314343214324432512322245112324313433244233124252444311344443215

Repetition de 1 : 14

" 2 : 21

" 3 : 21

" 4 : 21

" 5 7

Le nombre sera : 2+3+4 = 9

Le 4e code est 9

Etape 5 : CHIFFREMENT DE Vigenère

Pour cette partie, j'ai utilisé le programme vigenere_gui.py afin de retrouver la clé utilisée pour chiffrer le message.
L'objectif était de déterminer la longueur de la clé, les décalages entre les colonnes, et finalement de déduire la clé exacte.

J'ai d'abord commencé ma réflexion avec le test Kasiski qui a donné le résultat ci-dessous. J'en ai déduit que la clé était de longueur 3, mais lorsque j'ai fait le test dans le code donné dans l'énoncé, j'ai vite remarqué que ça n'avait pas de sens. j'ai donc continué mon essai avec 4 et 5 (mais je n'ai rien trouvé intéressant) comme avec la technique de Friedman dans le cours.

UPVUNEQYWJYLDIJSOZZDVCODAQVPNFGNVELZEGVUFZSRVUDRUTIKMSQELEILBHVRFRUWZTUIQHZ
IYIOIKGHFZGVGNAQWGGLVCYVXILEIE COIQDRWNRZXRFYTTMWHLVDIKEBZRJIGLCQWUKZWQVVPNJ
YIJUUXQWAGMLUWMTUZYIEVZZQVUGPFGWACDFGXVUCDBPVOYEFULGFHGIJNCXZIJRILDECNIESII
NYKQBKGGRUWAGNZQRJCFVDIGGNVDNVUOZEZICCDQRKHCVDHVXILENVNYJAYCKAEQEEQOMQ
ELRILDULGGFZQVUMRSIJQCKNMVPWCMMIQOZVIJWCJRMVTXVHSLUFVEKRTMVFPVUAFE

CO	84	2,3,7
VU	36	2,3
VPN	120	2,3,5
LEI	45	3,5
WAG	78	2,3 13

Mais à la longueur 6 j'ai trouvé le résultat suivant :

IC(Y(0))= 0.087978 ,IC(Y(1))= 0.067797 ,IC(Y(2))= 0.131073 ,IC(Y(3))= 0.074011, IC(Y(4))= 0.062147
IC(Y(5))= 0.072316

En observant les valeurs de l'indice de coïncidence pour plusieurs tailles, j'ai remarqué que pour k = 6, les valeurs se rapprochaient fortement de celles attendues pour un texte en français (autour de 0.07 à 0,13) que pour k=3 que je pensais correct de base.
C'est ce qui m'a permis de conclure que la clé possédait 6 lettres.

Déduisons la clé avec K= 6

Une fois la longueur confirmée, j'ai utilisé la fonction IC(x,y−k) du programme.
Pour chaque paire de colonnes en gardant x=0 comme référence, j'ai fait varier y de 1 à 5.
Le programme affichait 26 valeurs correspondant à chaque décalage possible, et j'ai noté à chaque fois la valeur de k pour laquelle l'indice de coïncidence était le plus élevé.

En procédant ainsi, j'ai observé les décalages suivants : Pour (x=0, y=1), le maximum se trouvait à k=18. Pour (x=0, y=2), à k=5. Pour (x=0, y=3), à k=16.Pour (x=0, y=4), à k=8.Et pour (x=0, y=5), à k=5.

Ces résultats signifient que les colonnes du texte chiffré sont décalées respectivement de ces valeurs les unes par rapport aux autres. Cela m'a permis d'établir la relation entre les lettres de la clé : chaque lettre suivante est obtenue en ajoutant ce décalage à la première, modulo 26**.**

Ensuite, j'ai utilisé la dernière partie du programme, Fréquences dans Y(x), pour chaque colonne du texte. Cette fonction affiche la fréquence des lettres dans chaque sous-texte correspondant à une position fixe dans la clé. Voici ce que j'ai observé pour les lettres les plus fréquentes :Dans la colonne

0 la lettre qui apparaissait le plus souvent est q et dans la colonne 1 c'était i. Dans la colonne 2 j'ai obtenu v. Dans la colonne 3 c'était g dans la colonne 4 c'était n.et dans la colonne 5 c'était z.

En français, la lettre la plus fréquente est généralement E, donc j'ai fait l'hypothèse que, dans la première colonne, la lettre la plus fréquente du texte chiffré correspondait à un E dans le texte clair.

En me basant sur cette hypothèse, j'ai cherché la valeur de la première lettre de la clé.
Dans l'alphabet, la lettre Q correspond à l'indice 16 et la lettre E à l'indice 4.
Le décalage entre les deux est donc de 12, ce qui correspond à la lettre M.
C'est la première lettre de la clé.

En ajoutant ensuite les décalages trouvés plus haut à cette première lettre, j'ai obtenu les suivantes, R, C, U et R.
La clé reconstituée est donc MERCUR.

Finalement en testant ma clé MERCUR j'ai obtenue le message en clair suivant :

ILESTNEUFHEURESQUINZEAUMOMENTOUJECRISCESLIGNESJAIPRISBEAUCOUPDEPLAISIRAREDIGERCE
TENONCEETJESPEREQUEVOUSENAUREZAUTANTADECHIFFRERETCHIFFRERLESDIFFERENTSMESSAGESJE
SUISVRAIMENTFIERDEVOUSJAJOUTESIMPLEMENTQUELQUESLIGNESPOURALLONGERLETEXTEMAISJET
IENSALEREPETERJESUISVRAIMENTFIERDEVOUSJELESOULIGNEANOUVEAUPOURQUEMONMESSAGESO
ITBIENCLAIROUIJESUISFIERDEVOUSLESGARSETLESGOS.

En faisant la somme de 9+15 =24 et ensuite 2+4 =6

Le cinquième code est donc 6

Et le code complet est :35296