IREM de Clermont-Ferrand
Formation algorithmique
STS SIO

Stage du 22 septembre 2011
Malika More
malika.more@u-clermont1.fr

Cryptographie en Python

Introduction Les méthodes de cryptographie dites *à clé secrète* ont été utilisées dans la vie réelle depuis l'Antiquité jusqu'à la seconde guerre mondiale. Si celles que nous présentons ici sont très simples, il en existe d'autres beaucoup plus élaborées. Mais on s'est aperçu qu'aucune d'entre elles ne résiste bien longtemps face à la puissance de calcul apportée par les ordinateurs. C'est pourquoi elles ont été en général abandonnées et remplacées par des méthodes plus sûres et radicalement différentes, dites *à clé publique*, comme la méthode RSA, très largement utilisée sur internet pour la sécurité des transactions et des échanges.

L'intérêt d'étudier quelques techniques anciennes est qu'elles font travailler sur le calcul modulaire en maths, et utiliser de nombreuses notions du programme en algorithmique.

Vocabulaire

- La *Cryptologie* est la science des messages secrets. Elle se décompose en deux disciplines :
  - ⋆ la *Cryptographie*, art de transformer un message clair en un message inintelligible par celui qui ne possède pas la clé de déchiffrement. Cependant, on utilise souvent le mot cryptographie comme synonyme de cryptologie.
  - ⋆ la *Cryptanalyse*, art d'analyser un message chiffré afin de le décrypter quand on ne posséde pas la clé de déchiffrement.
- Chiffre : anciennement code secret, par extension désigne aussi un algorithme utilisé pour le chiffrement ;
- Chiffrer : transformer à l'aide d'une clé de chiffrement un message en clair en un message chiffré, incompréhensible si on ne dispose pas de la clé de déchiffrement correspondante ;
- Déchiffrer : retrouver à l'aide de la clé de déchiffrement correspondante le message en clair d'origine à partir d'un message précédemment chiffré à l'aide d'une clé de chiffrement ;
- Clé de chiffrement : méthode permettant de chiffrer un message en clair ;
- Clé de déchiffrement : méthode associée à une clé de chiffrement et permettant de déchiffrer un message précédemment chiffré ;
- Décrypter : retrouver le message en clair correspondant à un message chiffré sans posséder la clé de déchiffrement ni la clé de chiffrement ;
- Cryptogramme : message chiffré (incompréhensible si on ne dispose pas de la bonne clé de déchiffrement).

Consignes générales

- On écrit les messages en lettres majuscules et sans accents. Ceci a pour but de simplifier le chiffrement et le déchiffrement des messages.
- Lorsque les messages sont constitués de plusieurs mots ou de plusieurs phrases, on conserve les espaces entre les mots et les signes de ponctuation. Le résultat est de faciliter encore le déchiffrement.
- Ce n'est pas conforme à la réalité, puisque dans la vraie vie, on veut au contraire compliquer au maximum le cryptogramme, pour empêcher l'adversaire de le décrypter, si possible...

- Plus un cryptogramme est long, plus il est facile à décrypter, car l'adversaire dispose de plus d'indices. Ceci explique pourquoi, dans les exercices, les messages à décrypter seront significativement plus longs que les messages à chiffrer ou à déchiffrer.
- On utilise la correspondance ci-dessous entre les lettres de l'alphabet $\{A, B, C, \ldots, Z\}$ et les nombres $\{0, 1, 2, \ldots, 25\}$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

1 Chiffrement par décalage

- Un chiffrement par décalage consiste à décaler les lettres de l'alphabet d'une valeur fixe.
- Et bien sûr, si on dépasse Z, on reprend à partir de A.
- Autrement dit, on travaille « modulo 26 ».

Exercice 1 (Chiffre de César)**.** Les lettres de l'alphabet sont chiffrées à l'aide de la clé de chiffrement :

$$f : \left\{ \begin{array}{ccc} \{0,1,\ldots,25\} & \longrightarrow & \{0,1,\ldots,25\} \\ x & \mapsto & f(x) = x+4 \mod 26 \end{array} \right.$$

Cette méthode est réputée avoir été utilisée par Jules César pour communiquer secrètement avec ses généraux pendant la guerre des Gaules, d'où son nom.

1. Chiffrer le message : ALLEZ-Y.
2. Quelle est la clé de déchiffrement du chiffre de César ?
3. Déchiffrer la réponse du général : SR C ZE

Exercice 2 (Une faiblesse dangereuse)**.** Combien y-a-t-il de chiffrements par décalage différents ?

Exercice 3 (Une faille de sécurité)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement par décalage inconnu : TZTVIFE VJK LE REV. Un espion habile a réussi à découvrir que la lettre S est chiffrée par la lettre J.

1. Décrypter le message proposé.
2. Préciser quelles sont les clés de chiffrement et de déchiffrement correspondantes.

Exercice 4 (Décryptage)**.** Le cryptogramme suivant a été obtenu é l'aide d'un chiffrement par décalage inconnu :

TOX VXLTK !
C'TB VTIMNKX NG XLIBHG.
T UBXGMHM,
LBZGX : FTKV-TGMHBGX

1. Proposer deux méthodes de décryptage (impliquant éventuellement l'utilisation d'un ordinateur), l'une tirant parti de l'exercice 2, et l'autre de l'exercice 3.
2. Décrypter le message proposé.
3. Préciser quelles sont les clés de chiffrement et de déchiffrement correspondantes.

Exercice 5 (Programmation)**.** Dans le fichier `DecalageQuestion.py`, les fonctions techniques `Decale`, `CleDechiffre`, `BruteForce` et `Espion` permettant de faire fonctionner les procédure de chiffrement, déchiffrement et décryptage d'un code par décalage ont été sabotées. Pouvez-vous les réparer ? Les solutions se trouvent dans le fichier `DecalageReponse.py`

2 Intermède : Inverse modulaire

Définition. Soit $n \geq 2$ un entier naturel, et soit $a \in \mathbb{Z}/n\mathbb{Z}$.
- On dit que a est inversible modulo n lorsqu'il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab \equiv 1 \mod n$.
- Lorsqu'il existe, le nombre b est unique, s'appelle l'inverse modulaire de a, et se note $a^{-1} \mod n$.

Exemple.
7 est inversible modulo 10 car $7 \times 3 = 21$ i.e.

$$7 \times 3 \equiv 1 \mod 10$$

Et l'inverse de 7 modulo 10 est 3

Propriétés.
- Le nombre a est inversible modulo n si et seulement si a est premier avec n.
- Le nombre a est inversible modulo n si et seulement si il existe des coefficients de Bézout u et v tels que $au + nv = 1$. Dans ce cas, u est congru modulo n à l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$
- Si p est premier, alors tous les nombres non nuls dans $\mathbb{Z}/p\mathbb{Z}$ sont inversibles modulo p.
- Quel que soit $n \geq 2$, les nombres 1 et $n-1$ sont inversibles modulo n, et on a $1^{-1} \equiv 1 \mod n$ et $(n-1)^{-1} \equiv n-1 \mod n$.

Utilisation Résoudre l'équation $7x \equiv 4$ dans $\mathbb{Z}/10\mathbb{Z}$
- J'ai besoin de l'inverse de 7 modulo 10 : c'est 3, comme on vient de le voir
- Je pars de : $7x \equiv 4 \mod 10$
- Je multiplie par $7^{-1} \mod 10$ les deux membres de l'équation : $3 \times (7x) \equiv 3 \times 4 \mod 10$
- Je regroupe : $(3 \times 7)x \equiv 12 \mod 10$
- Je simplifie « modulo 10 » : $1x \equiv 2 \mod 10$
- Finalement j'arrive à : $x \equiv 2 \mod 10$

Remarque. Lorsque a n'est pas inversible modulo n, l'équation $ax = b$ ne possède pas une solution unique dans $\mathbb{Z}/n\mathbb{Z}$ (elle peut avoir plusieurs solutions, ou bien aucune solution, selon les valeurs de a, b, n).

Calcul de l'inverse de a modulo n
- À la main, comme dans l'exemple ci-dessus
- Méthode exhaustive : en particulier si n est petit ou si on dispose d'un ordinateur
- Recherche des coefficents de Bézout en utilisant l'algorithme d'Euclide étendu

L'algorithme d'Euclide étendu

Exemple. Calcul du pgcd de 546 et 495 en utilisant l'algorithme d'Euclide :

$$\begin{array}{lllllll} 546 & - & 495 & \times & 1 & = & 51 \\ 495 & - & 51 & \times & 9 & = & 36 \\ 51 & - & 36 & \times & 1 & = & 15 \\ 36 & - & 15 & \times & 2 & = & 6 \\ 15 & - & 6 & \times & 2 & = & 3 \\ 6 & - & 3 & \times & 2 & = & 0 \end{array}$$

On a $PGCD(546, 495) = 3$, donc il existe des entiers u et v tels que $546 \times u + 495 \times v = 3$.
Pour trouver des nombres u et v qui vérifient cette propriété, on étend les calculs de l'algorithme

d'Euclide :

		546			1			0
		495			0			1
$546 - 495 \times 1$	$=$	51	$1 - 0 \times 1$	$=$	1	$0 - 1 \times 1$	$=$	-1
$495 - 51 \times 9$	$=$	36	$0 - 1 \times 9$	$=$	-9	$1 - (-1) \times 9$	$=$	10
$51 - 36 \times 1$	$=$	15	$1 - (-9) \times 1$	$=$	10	$-1 - 10 \times 1$	$=$	-11
$36 - 15 \times 2$	$=$	6	$-9 - 10 \times 2$	$=$	-29	$10 - (-11) \times 2$	$=$	32
$15 - 6 \times 2$	$=$	3	$10 - (-29) \times 2$	$=$	68	$-11 - 32 \times 2$	$=$	-75
$6 - 3 \times 2$	$=$	0						

On trouve $u = 68$ et $v = -75$ (Rappel : ils ne sont pas uniques).
Autrement dit on a

$$546 \times 68 + 495 \times (-75) = 3$$

Preuve On calcule simultanément le pgcd de a et de b et un couple de coefficients de Bézout, entiers relatifs (u, v) tels que $a \times u + b \times v = \text{pgcd}(a, b)$

q	r	u	v
	$r_0 = a$	$u_0 = 1$	$v_0 = 0$
	$r_1 = b$	$u_1 = 0$	$v_1 = 1$
$q_2 = \text{quo}(r_0, r_1)$	$r_2 = r_0 - r_1 \cdot q_2$	$u_2 = u_0 - u_1 \cdot q_2$	$v_2 = v_0 - v_1 \cdot q_2$
$\dots$	$\dots$	$\dots$	$\dots$
$q_{i+1} = \text{quo}(r_{i-1}, r_i)$	$r_{i+1} = r_{i-1} - r_i \cdot q_{i+1}$	$u_{i+1} = u_{i-1} - u_i \cdot q_{i+1}$	$v_{i+1} = v_{i-1} - v_i \cdot q_{i+1}$
$\dots$	$\dots$	$\dots$	$\dots$
$q_n = \dots$	$r_n = \dots$	$u_n = \dots$	$v_n = \dots$
$q_{n+1} = \dots$	$r_{n+1} = 0$		

Vérifions qu'on a $r_n = \text{pgcd}(a, b)$ et $a \times u_n + b \times v_n = r_n$.
La colonne des r correspond à l'algorithme d'Euclide ordinaire, donc on a bien $r_n = \text{pgcd}(a, b)$, puisque c'est le dernier reste non nul.
On a $a \times u_0 + b \times v_0 = a = r_0$ et $a \times u_1 + b \times v_1 = b = r_1$. Puis on vérifie par récurrence que pour tout $i > 0$, si on a $a \times u_{i-1} + b \times v_{i-1} = r_{i-1}$ et $a \times u_i + b \times v_i = r_i$, alors on a $a \times u_{i+1} + b \times v_{i+1} = r_{i+1}$.
Finalement, on a bien $a \times u_n + b \times v_n = r_n$.

3 Chiffrement affine

- Un chiffrement affine consiste à utiliser comme clé de chiffrement une fonction affine :

$$f : \left\{ \begin{array}{ccc} \{0,1,\ldots,25\} & \longrightarrow & \{0,1,\ldots,25\} \\ x & \mapsto & f(x) = ax + b \mod 26 \end{array} \right.$$

  (où a et b sont des entiers).
- Un chiffrement par décalage correspond à un cas particulier pour lequel $a = 1$.

Exercice 6 (Chiffrer/Déchiffrer)**.** On chiffre les lettres de l'alphabet à l'aide de la clé de chiffrement :

$$f : \left\{ \begin{array}{ccc} \{0,1,\ldots,25\} & \longrightarrow & \{0,1,\ldots,25\} \\ x & \mapsto & f(x) = 17x + 22 \mod 26 \end{array} \right.$$

1. Chiffrer le message : TEST.
2. La clé de déchiffrement correspondante est :

$$g : \left\{ \begin{array}{ccc} \{0,1,\ldots,25\} & \longrightarrow & \{0,1,\ldots,25\} \\ x & \mapsto & g(x) = 23x + 14 \mod 26 \end{array} \right.$$

   Vérifiez-le en déchiffrant le message que vous avez chiffré à la question 1.
3. Déchiffrer le message : NZWPA.

- Contrairement au cas des chiffrements par décalage, ici le calcul de la clé de déchiffrement correspondant à une clé de chiffrement donnée n'est pas immédiat.
- C'est l'objet de l'exercice 7.
- Par ailleurs, toutes les clés de chiffrement affines ne sont pas correctes, c'est l'objet de l'exercice 8.

Exercice 7 (Calculer la clé de déchiffrement)**.**

1. Pour les clés de chiffrement et de déchiffrement de l'exercice 6, calculer $g(f(x)) \mod 26$. Expliquer le résultat.
2. On considére la clé de chiffrement affine $f(x) = ax + b \mod 26$ et la clé de déchiffrement associée $g(x) = a'x + b' \mod 26$. Calculer $g(f(x)) \mod 26$. En déduire les relations que doivent vérifier (a, b) et (a', b') ?
3. On considére la clé de chiffrement $f(x) = 7x + 8$. Déterminer l'inverse de 7 modulo 26, puis calculer la clé de déchiffrement $g(x)$ associée.
4. On choisit $a = 9$ et $b = 13$. Déterminer deux entiers u et v tels que $au + 26v = 1$, et en déduire a' puis b'.

Exercice 8 (Une mauvaise clé)**.** Un cryptographe peu averti décide d'utiliser la clé de chiffrement affine :

$$f : \left\{ \begin{array}{ccc} \{0,1,\ldots,25\} & \longrightarrow & \{0,1,\ldots,25\} \\ x & \mapsto & f(x) = 6x + 5 \mod 26 \end{array} \right.$$

1. Déterminer le tableau de substitution des lettres correspondant à cette clé de chiffrement.
2. Expliquer pourquoi cette clé de chiffrement n'est pas correcte.
3. Pourquoi ne peut-on pas déterminer la clé de déchiffrement associée ?
4. Quels sont les nombres a qui, comme $a = 6$, ne peuvent pas servir à définir une clé de chiffrement affine $f(x) = ax + b \mod 26$ correcte ?

Exercice 9 (C'est encore faible)**.** Combien y-a-t-il de chiffrements affines différents ?

Exercice 10 (Il y a aussi une faille de sécurité)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement affine $f(x) = ax + b$ inconnu : THPPBXH PHRUHK. Un espion habile a réussi à découvrir que la lettre K est chiffrée par la lettre D, et que la lettre N est chiffrée par la lettre O.

1. Quelles informations sur a et b peut-on en déduire ?
2. Calculer la clé de chiffrement utilisée.
3. En déduire la clé de déchiffrement correspondante.
4. Décrypter le message proposé.
5. Trouver toutes les solutions (modulo 26) de l'équation $6a = 14$.
6. Tous les couples de lettres décryptées tels que $K \rightsquigarrow D$ et $N \rightsquigarrow O$ peuvent-ils convenir pour décrypter un cryptogramme affine ?

Exercice 11 (Décryptage)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement affine inconnu :

> FCI QHAVVPCYCRBI EVVARCI IKRB VEQAFCI E JCQPSDBCP E QKRJABAKR JC JAIDKICP J'UR QPSDBKOPEYYC PCFEBANCYCRB FKRO DKUP S BPKUNCP EIICL J'ARJAQCI.

1. Que deviennent les méthodes de décryptage envisagées dans le cas des chiffrements par décalage ?
2. Proposer deux méthodes de décryptage (impliquant éventuellement l'utilisation d'un ordinateur), l'une tirant parti de l'exercice 9, et l'autre de l'exercice 10.
3. Décrypter le message proposé.
4. Préciser quelles sont les clés de chiffrement et de déchiffrement correspondantes.

Exercice 12 (Programmation)**.** Sur le modèle de ce qui a été fait pour les codes par décalage, écrire en `Python` les fonctions techniques `Affine`, `CleDechiffre`, `BruteForce` et `Espion` et les procédures `Chiffrer`, `Dechiffrer`, `DecrypterEspion` et `DecrypterBrute` permettant de faire fonctionner et de décrypter un code affine. Les solutions se trouvent dans le ficher `Affine.py`.

4 Approfondissement : Le chiffre de Hill

Cette partie présente un chiffre inventé en 1929 par un mathématicien américain, Lester Hill.

- Pour chiffrer un message, on utilise la méthode suivante :
  - On découpe le message écrit en clair en groupes de 2 lettres.
  - On rappelle la correspondance habituelle entre les lettres de l'alphabet $\{A, B, C, \ldots, Z\}$ et les nombres $\{0, 1, 2, \ldots, 25\}$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

  - Pour chaque couple de nombres (x_1, x_2), on calcule un nouveau couple (y_1, y_2) en utilisant une **clé de chiffrement**, disons pour cette question $\begin{cases} y_1 = 2x_1 + 5x_2 \mod 26 \\ y_2 = x_1 + 3x_2 \mod 26 \end{cases}$.
  - On remplace chaque couple de nombres obtenus par les deux lettres correspondantes dans le tableau.
  - On rassemble tous les groupes de deux lettres pour obtenir le cryptogramme.
- Pour déchiffrer un cryptogramme, on utilise la même méthode, en remplaçant la clé de chiffrement par la **clé de déchiffrement** correspondante, qui est dans notre cas $\begin{cases} x_1 = 3y_1 + 21y_2 \mod 26 \\ x_2 = 25y_1 + 2y_2 \mod 26 \end{cases}$.

Exercice 13 (Chiffrer/Déchiffrer)**.**

1. Quel est le cryptogramme obtenu à partir du mot **CRYPTO** ?
2. Vérifiez que la clé de déchiffrement qui vous a été fournie est correcte.

3. Pouvez-vous déchiffrer le cryptogramme **CDAWYQGF** ?

Exercice 14 (Sécurité du chiffre de Hill)**.** On s'inspire de la méthode suivie dans le cas des chiffrements affines.

1. Combien y-a-t-il au maximum de chiffres de Hill différents ? On ne vous demande pas le nombre précis, mais un majorant assez simple.
2. Le cryptogramme suivant a été obtenu à l'aide d'un chiffre de Hill $\begin{cases} y_1 = ax_1 + bx_2 \mod 26 \\ y_2 = cx_1 + dx_2 \mod 26 \end{cases}$ inconnu : HQZV. Un espion habile a réussi à découvrir que le couple (C ;B) est chiffré par le couple (N ;J), et que le couple (F ;D) est chiffré par le couple (K ;Z). Pouvez-vous décrypter le message proposé ?
3. Question plus difficile : Tous les couples de couples de lettres décryptées tels que $(C;B) \rightsquigarrow (N;J)$ et $(F;D) \rightsquigarrow (K;Z)$ peuvent-ils convenir pour décrypter un cryptogramme de Hill ?
4. Que concluez-vous à propos de la sécurité de la méthode de Hill ?
5. Le cryptogramme suivant a été obtenu à l'aide d'un chiffre de Hill inconnu :
   MTLJZGGMX ! FU TIKM XIKHLX ZXDKD TZUA-OOOO KV CNODRGI PQ TAJJ ZYXUD ZH OORMATG BRNDHEGI PANA EOF WJKDEOWK, FTUA HLG UWML-JOOW PG OUDHTCZDAUDH UKS QUEWG OHL DN CNODRGAYCZT. AIKA RIKZPX ZUDIVMTKD KWL KME WJAYXEME JKYFEIME WQ'UD E PFHG UKYT QG OZJO-QMP HLA ECUTUIAMCZGC FO FYXHL YQBSI CA'QJZ ZPFHZXCZR ZVR XDZHT-NUD XLCZ BTBSIAGTMCXD. VJXF HLW CWBXDA EKS, ZH KRI PI PGONDTUX-DOOZG QUXQMEDHTQANLJ MEF GCMOKIKF INBA ESCXEKOSMG À OWLCAHLX, DH UIRLDOQ V'RVZIVG BKS JD FTWB.
   Pouvez-vous décrypter le message proposé ? Décrivez la méthode que vous avez utilisée.

Exercice 15 (Fabrication d'un couple de clés de Hill)**.**

Remarque. Cet exercice est formulé pour des étudiants qui n'ont pas encore vu les matrices.

1. Montrer que le système $\begin{cases} y_1 = 6x_1 + 2x_2 \mod 26 \\ y_2 = 2x_1 + 1x_2 \mod 26 \end{cases}$ ne correspond pas à une clé de chiffrement valide.
2. Vérifier que les systèmes $\begin{cases} y_1 = 2x_1 + 5x_2 \mod 26 \\ y_2 = x_1 + 3x_2 \mod 26 \end{cases}$ et $\begin{cases} y_1 = 2x_1 + 5x_2 \mod 26 \\ y_2 = x_1 + 3x_2 \mod 26 \end{cases}$ constituent un couple de clés de chiffrement/déchiffrement valide.
3. On considère les systèmes $\begin{cases} y_1 = ax_1 + bx_2 \mod 26 \\ y_2 = cx_1 + dx_2 \mod 26 \end{cases}$ et $\begin{cases} Y_1 = dX_1 + -bX_2 \mod 26 \\ Y_2 = -cX_1 + aX_2 \mod 26 \end{cases}$.
   Calculer le résultat (Y_1, Y_2) de l'application du second système au résultat obtenu en appliquant le premier système sur un couple (x_1, x_2).
4. En déduire une condition sur a, b, c, d pour que le premier système $\begin{cases} y_1 = ax_1 + bx_2 \mod 26 \\ y_2 = cx_1 + dx_2 \mod 26 \end{cases}$ soit une clé de chiffrement valide, autrement dit pour qu'une clé de déchiffrement associée existe.
5. Lorsque le système $\begin{cases} y_1 = ax_1 + bx_2 \mod 26 \\ y_2 = cx_1 + dx_2 \mod 26 \end{cases}$ constitue une clé de chiffrement valide, quelle est la clé de déchiffrement associée ?
6. Déterminer la clé de déchiffrement correspondant à la clé de chiffrement proposée dans les cas suivants :
   $\begin{cases} y_1 = 3x_1 + x_2 \mod 26 \\ y_2 = 2x_1 + x_2 \mod 26 \end{cases}$ $\begin{cases} y_1 = 2x_1 + x_2 \mod 26 \\ y_2 = x_1 + 3x_2 \mod 26 \end{cases}$ $\begin{cases} y_1 = 3x_1 + 3x_2 \mod 26 \\ y_2 = 5x_1 + 8x_2 \mod 26 \end{cases}$
7. Dans chaque cas, vérifiez si la clé de déchiffrement que vous avez proposée est correcte.
8. Fabriquer un couple valide de clés de chiffrement/déchiffrement, et vérifier que c'est bien le cas.

Exercice 16 (Généraliser le chiffre de Hill)**.** Au lieu de grouper les lettres des messages 2 par 2, on peut les grouper 3 par 3, ou plus généralement k par k, et utiliser un système linéaire de k équations à k inconnues (modulo 26) en guise de clé de chiffrement.
Donner un majorant simple du nombre de chiffre différents possibles en fonction de k.

Exercice 17 (Programmation)**.** La programmation des fonctions techniques permettant de faire fonctionner et de décrypter un code de Hill est plus délicate que dans le cas des chiffrements par décalage et des chiffrements affines, mais vous pouvez vous y essayer. Les solutions se trouvent dans le fichier `Hill.py`.

5 Partie facultative : Chiffrement par substitution

- Un chiffrement par substitution simple consiste à remplacer chaque lettre par une autre, selon une méthode décidée à l'avance.
- Un chiffrement affine correspond à un cas particulier où la substitution se calcule à l'aide d'une fonction affine.
- Les chiffrement par subsitution ne font pas appel au calcul modulaire, mais la méthode de décryptage basée sur l'analyse des fréquences présente un intérêt culturel.

Exercice 18 (Chiffrer/Déchiffrer)**.** Dans le cas général, il n'y a pas de fonction mathématique simple permettant de chiffrer chaque lettre, c'est pourquoi on donne la table de chiffrement en entier. On utilise la substitution suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
S	C	W	U	D	X	B	F	Y	T	G	Z	I

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	O	J	N	K	A	M	L	P	E	Q	R	V

1. Chiffrer le message : FACILE.
2. Écrire la table de déchiffrement correspondante.
3. Déchiffrer le message DAASY.

Exercice 19 (Cette fois, ce n'est pas faible)**.** Combien y-a-t-il de chiffrements par substitution simples différents ?

Exercice 20 (Décryptage)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement par substitution simple inconnu :

> RC IZQKOGJZCKVYD DTO SUD PDT PYTIYKRYUDT PD RC IZQKOGRGJYD T'COOCIVCUO C KZGODJDZ PDT XDTTCJDT (CTTSZCUO IGUBYPDUOYCRYOD, CSOVDUOYIYOD DO YUODJZYOD) DU T'CYPCUO TGSLDUO PD TDIZDOT GS IRDT. DRRD DTO SOYRYTDD PDKSYT R'CUOYWSYOD, XCYT IDZOCYUDT PD TDT XDOVGPDT RDT KRST YXKGZOCUODT, IGXXD RC IZQKOGJZCKVYD CTQXDOZYWSD, U'GUO WSD WSDRWSDT PYMCYUDT P'CUUDDT P'DHYTODUID. AYDU WS'DXYUDXXDUO TOZCODJYWSD, RC IZQKOGJZCKVYD DTO ZDTODD KDUPCUO OZDT RGUJODXKT SU CZO, KGSZ UD PDLDUYZ SUD TIYDUID WS'CS HHD TYDIRD. CLDI R'CKKCZYOYGU PD R'YUBGZXCOYWSD, TGU SOYRYTCOYGU TD PDXGIZCOYTD PD KRST DU KRST.

1. Que deviennent les méthodes de décryptage utilisées précédemment ?
2. Décrypter le message proposé.
3. Décrire la méthode utilisée.