TP 2 – Chiffrement affine

On se donne a et b deux entiers non nuls.
On définit le chiffrement affine de paramètres a et b de la manière suivante :

- Chaque lettre du texte à chiffrer est associée à un entier x entre 0 et 125 selon la correspondance du code ASCII (voir annexe).
- A chaque entier x, on associe l'entier y tel que $\begin{cases} y \equiv ax + b\,[256] \\ 0 \leqslant y \leqslant 255 \end{cases}$.
- On remplace la lettre du message par la lettre correspondant au nombre y.

L'objectif du TP est de chiffrer puis de déchiffrer le texte suivant d'Henri Poincaré publié en 1908 dans *Science et méthode* :

« La mathématique est l'art de donner le même nom à des choses différentes. »

Partie A - Questions mathématiques préliminaires

On se donne un nombre y que l'on souhaite déchiffrer (c'est-à-dire retrouver la valeur de x initiale).

1. A quelle condition sur a est-il possible de déterminer une unique valeur de x telle que $y \equiv ax + b\,[256]$?
2. Dans le cas où a est inversible modulo 256, on note m son inverse. Déterminer la valeur de x en fonction de y, b et m.

   Dans toute la suite du TP, on considère le cas où $a = 15$ et $b = 112$.
3. Écrire un algorithme Python permettant de montrer que 15 est inversible modulo 256 et de déterminer son inverse.

Partie B - Transformation du texte en une liste de nombres

1. Créer une chaîne de caractères contenant le texte à chiffrer.

2. Créer une liste, nommée ListeInitiale, contenant les nombres x correspondant au texte à chiffrer.

Partie C - Chiffrement et déchiffrement

1. **Chiffrement.**
   (a) Créer une liste, nommée ListeChiffree, contenant les nombres y calculés à partir des nombres x.
   (b) Convertir la liste précédente en une chaîne de caractères, nommée Chiffre, afin d'obtenir le message chiffré.
2. **Déchiffrement.**
   Écrire un algorithme permettant de déchiffrer la liste ListeChiffree afin de retrouver le message initial de Poincaré.
3. Quels sont, à votre avis, les limites du procédé de chiffrement affine ?

Histoire

Henri Poincaré (1854-1912) est un mathématicien français. Il est souvent considéré comme le dernier savant universel de l'Histoire au sens où il conaissait tous les domaines des mathématiques de son époque ainsi que de nombreux domaines de la physique. Il a notamment écrit plusieurs ouvrages de vulgarisation scientifiques, dont *La Science et l'Hypothèse* en 1902, *La Valeur de la Science* en 1905 ou encore *Science et méthode* en 1908.

Henri Poincaré

Annexe – code ASCII

Au début de l'informatique, chaque ordinateur avait son propre système d'encodage. Il existait un besoin de standardisation et *l'American Standard Code for Information Interchange* (ASCII) a alors été créé dans les années 1960. Le code ASCII a été défini comme norme en 1975. Il contient 128 caractères, numérotés de 0 à 127 (ils sont donc codés par 7 bits). Le tableau ci-dessous donne la correspondance du code et des caractères.

Ayant été créé aux États-Unis, le code ASCII ne contient pas de caractères accentués. Dans les pays latins, il a donc été remplacé par un autre code, appelé code ASCII étendu. Ce code contient 256 caractères soit le double du code ASCII original. Depuis 2007, cette norme a été remplacée par Unicode (UTF-8) qui offre plus de possibilités.

En Python, il est possible de convertir un caractère en son code ASCII et réciproquement (dans le code ASCII étendu). Pour cela on utilise les fonctions Python **ord** et **chr**.

Table ASCII 7 bits

Code	Car.	Code	Car.	Code	Car.	Code	Car.	Code	Car.	Code	Car.	Code	Car.	Code	Car.
000	NULL	016	DLE	032	Space	048	0	064	@	080	P	096	‘	112	p
001	SOH	017	DC1	033	!	049	1	065	A	081	Q	097	a	113	q
002	STX	018	DC2	034	"	050	2	066	B	082	R	098	b	114	r
003	ETX	019	DC3	035	#	051	3	067	C	083	S	099	c	115	s
004	EOT	020	DC4	036	$	052	4	068	D	084	T	100	d	116	t
005	ENQ	021	NAK	037	%	053	5	069	E	085	U	101	e	117	u
006	ACK	022	SYN	038	&	054	6	070	F	086	V	102	f	118	v
007	BELL	023	ETB	039	'	055	7	071	G	087	W	103	g	119	w
008	BS	024	CAN	040	(	056	8	072	H	088	X	104	h	120	x
009	TAB	025	EM	041	)	057	9	073	I	089	Y	105	i	121	y
010	LF	026	SUB	042	*	058	:	074	J	090	Z	106	j	122	z
011	VT	027	FSC	043	+	059	;	075	K	091	[	107	k	123	{
012	FF	028	FS	044	’	060	<	076	L	092	\	108	l	124	|
013	CR	029	GS	045	-	061	=	077	M	093	]	109	m	125	}
014	SO	030	RS	046	.	062	>	078	N	094	ˆ	110	n	126	˜
015	SI	031	US	047	/	063	?	079	O	095	_	111	o	127	DEL