Exercice : La cryptographie symétrique

Exercice 1

On rappelle que le OU exclusif XOR se note par un accent circonflexe en python : $4 \oplus 5 = 4\hat{}5$.

1) On veut calculer 154ˆ45.

a) Calculer dans une console Python la valeur 154ˆ45.

b) Transformer chaque nombre en binaire puis appliquer l'opérateur logique xor bit à bit.

c) Les valeurs trouvées sont-elles égales ?

2) Calculer en Python $Aˆz$. Expliquer la valeur obtenue et donner le caractère ASCII associé.

Exercice 2

1) Écrire la fonction chiffrer(msg,cle) qui a 2 paramètres, msg une chaine de caractères qui est le message à chiffrer et cle qui est la clef de chiffrement. Cette fonction renvoie une chaine de caractères correspondant au mot chiffré avec l'opérateur XOR.

Si la clef de chiffrement est plus courte que le message à chiffrer, celle-ci est répétée jusqu'à la fin du message.

2) Chiffrer le message BONJOUR avec la clef de chiffrement 12xy.

3) Déchiffrer votre message chiffré et vérifier qu'on obtient bien le message initial.

Exercice 3

On peut écrire un programme qui met en place les conditions du chiffrement de Vernam.
On convertira les chaines de caractères en binaire avec la fonction bytes. Cette fonction a 2 paramètres :

— Le premier paramètre est la chaine de caractères constituant le message à convertir en binaire.

— Le second paramètre est l'encodage à utiliser.

Exemples :

— bytes('bonjour','utf8') donne b'bonjour'

— bytes('bonjour','latin1') donne b'bonjour'

— bytes('lycée','utf8') donne b'lyc\xc3\xa9e'

— bytes('lycée','latin1') donne b'lyc\xe9e'

1) Pourquoi y a-t-il une différence en convertissant le mot lycée et pas pour le mot bonjour ?

2) Écrire la fonction cle_alea qui prend en paramètre une longueur de message et renvoie une clé de chiffrement constitué de caractères imprimables choisis au hasard dans la table ASCII.

3) Écrire la fonction chiffrer(msg,cle) qui a 2 paramètres, msg une chaine de caractères qui est le message à chiffrer et cle qui est la clef de chiffrement. Cette fonction renvoie la chaine de caractères correspondant au message chiffré avec l'opérateur XOR et la clé de chiffrement utilisée. Cette fonction suit l'algorithme suivant :

— On crée une chaine binaire vide renvoyée par la fonction ;

— On convertit en binaire le message à chiffre ;

— On crée une clé de chiffrement aléatoire de même longueur que le message convertie en binaire ;

— Avec une boucle, on parcourt le message binaire et on lui applique le XOR avec la clé. Le résultat est concaténée à la chaine binaire à renvoyer ;

— On finit en renvoyant le message chiffré et la clé de chiffrement.

4) La fonction dechiffrer(msg,cle) a deux paramètres :

— Le message chiffré msg

— La clé de chiffrement utilisée pour chiffre le message.

Cette fonction renvoie le message chiffré en clair.
Écrire le code python de cette fonction.

5) Chiffrer le message 'La cryptographie symétrique est fantastique'. Vérifier ensuite que vous pouvez le déchiffrer.

6) Recommencer avec un message contenant des caractères spéciaux et accentués.

7) Que remarquez-vous si on utilise l'encodage UTF8 ?

Exercice 4

Pour chiffrer un message, une méthode dit du masque jetable, consiste à le combiner avec une chaîne de caractère de longueur comparable.
Une implémentation possible utilise l'opérateur XOR dont voici la table de vérité :

a	b	a XOR b
0	0	0
0	1	1
1	0	1
1	1	0

Dans la suite, les nombres écrits en binaire seront précédés du préfixe 0b.

1) Pour chiffre un message, on convertit chacun de ses caractères en binaire (à l'aide du format Unicode), et on réalise l'opération XOR bit à bit avec la clé.
Après conversion en binaire, et avant que l'opération XOR bit à bit avec la clé n'ait été effectuée, Alice obtient le message suivant :

$$m = \text{0b } 0110\ 0011\ 0100\ 0110$$

1) Le message m correspond à deux caractères codés chacun sur 8 bits : déterminer quels sont ces caractères. On fournit pour cela la table ci-dessous qui associe à l'écriture hexadécimale d'un octet le caractère correspondant.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	space	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

2) Pour chiffre le message d'Alice, on réalise l'opération XOR bit à bit avec la clé suivante :

$$k = \text{0b } 1110\ 1110\ 1111\ 0000$$

Donner l'écriture binaire du message obtenu.

3) **a)** Dresser la table de vérité de l'expression booléenne suivante :

(a XOR b) XOR b

b) Bob connaît la chaîne de caractères utilisée par Alice pour chiffrer le message. Quelle opération doit-il réaliser pour déchiffrer son message ?