Substitution monoalphabétique

Exercice 1 : Un chiffrement par décalage (César)
Vous décryptez le message suivant:

JL AFWL KL JVKL ZL JYHXBL MHJPSLTLUA

XOR Cipher

Exercice 2 :

1) Après un chiffrement XOR on obtient la message suivant : ri. Sachant que la clé de chiffrement est : 00001010 (la clé est directement donnée en binaire), déterminez le message d'origine.

On donne l'extrait de la table ASCII suivant :

lettre	code binaire	lettre	code binaire
a	01100001	t	01110100
b	01100010	v	01110110
c	01100011	w	01110111
d	01100100	x	01111000
e	01100101	y	01111001
f	01100110	z	01111010
i	01101001	| (vertical bar)	01111100
r	01110010	{ (left opening brace)	01111101
s	01110011	~ (tilde)	01111110

Exercice 3 :

Exercice tiré du bac 2021

Pour chiffrer un message, une méthode, dite du masque jetable, consiste à le combiner avec une chaîne de caractères de longueur comparable. Une implémentation possible utilise l'opérateur XOR (ou exclusif).

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

1) Pour chiffrer 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 = 0b 0110 0011 0100 0110

a) 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 (figure 2). Exemple de lecture : le caractère correspondant à l'octet codé 4A en hexadécimal est la lettre J.

	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

Figure 2

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

k = 0b 1110 1110 1111 0000

Donner l'écriture binaire du message obtenu.

2)

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 ?

Substitution monoalphabétique :
L'Atbash est un chiffrement par substitution monoalphabétique simple pour l'alphabet hébreu. Cette méthode de chiffrement substitue א (la première lettre) à ת (la dernière), ב (la deuxième) à ש (l'avant-dernière), et ainsi de suite, inversant l'alphabet.
Cette méthode de chiffrement est faible car il s'agit d'une simple substitution monoalphabétique. Cependant, au temps où l'Atbash était utilisé, faute d'outils mathématiques voire informatiques adaptés à la cryptologie, cela n'était pas spécialement un problème.

Le chiffrement Atbash adapté à l'alphabet latin serait :

En clair	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
Chiffré	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Substitution polyalphabétique (https://fr.wikipedia.org/wiki/Chiffre_de_Vigen%C3%A8re enigna)

Assimétrique

2) Un utilisateur B souhaite échanger un message chiffré avec un utilisateur A en utilisant un chiffrement asymétrique. A possède une clé publique (AKpub) et une clé privée (AKpriv). B possède une clé publique (BKpub) et une clé privée (BKpriv). B souhaite chiffrer un message m afin de pouvoir l'envoyer à A :

a) Quelle clé va être utilisée par B pour chiffrer le message m ?

b) Quelle clé va être utilisée par A pour déchiffrer le message m ?

3) Expliquez en quelques lignes le principe du protocole HTTPS (on s'intéressera uniquement à l'aspect Sécurité du protocole)