

Devoir maison

Exercice 1

Dans cette partie, pour une meilleure lisibilité, des espaces sont placées dans les écritures binaires des nombres. Il ne faut pas les prendre en compte dans les calculs.

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) 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.

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, on obtient le message suivant :

m = 0b 0110 0011 0100 0110

Le message m correspond à deux caractères codés chacun sur 8 bits :

Q1. 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

Pour chiffrer le message d'Alice, on réalise l'opération XOR bit à bit avec la clé suivante :
 $k = 0b\ 1110\ 1110\ 1111\ 0000$

Q2. Donner l'écriture binaire du message obtenu.

Q3. Dresser la table de vérité de l'expression booléenne suivante :
 $(a \text{ XOR } b) \text{ XOR } b$

Q4. Si l'on connaît la chaîne de caractères utilisée pour chiffrer le message. **Indiquer** l'opération à réaliser pour déchiffrer ce message.

Exercice 2

Cet exercice porte sur les bases de données relationnelles et le langage SQL. L'énoncé de cet exercice utilise les mots du langage SQL suivant :

SELECT, FROM, WHERE, JOIN, INSERT INTO, VALUES, COUNT, ORDER BY.

Dans un lycée imaginaire, les données relatives aux élèves de secondes sont regroupées dans un fichier nommé `seconde_lyc.csv`. Un extrait de son contenu est représenté figure 1.

num_eleve	nom	prenom	datenaissance	langue1	langue2	option	classe
133310FE	ACHIR	Mussa	01/01/2005	anglais	espagnol		2A
156929JJ	ALMEYER	Yohan	05/05/2005	allemand	anglais	théâtre	2D
500633KH	BELEY	Thibaut	05/05/2005	anglais	espagnol		2A
911887GA	BELEY	Marie	05/05/2005	anglais	espagnol		2A
906089JJ	BELEY	Manon	10/01/2005	anglais	allemand		2E
488697GA	CAILLE	Marie	30/03/2004	italien	anglais		2D
193514FB	CHARPENTIER	Jules	26/12/2005	espagnol	anglais		2C
321188FA	CLAUDEL	Benjamin	09/09/2005	espagnol	anglais		2E
081282GF	EISEN	Carla	23/06/2004	anglais	allemand		2A
026946KB	EL AYAR	Amir	11/09/2005	anglais	arabe	cinéma	2D
108303KG	GEHIN	Arthur	26/02/2005	allemand	anglais		2D
057934BK	GROSJEAN	Alexandre	09/11/2005	anglais	espagnol		2C
571113KE	HENRY	Paul	12/03/2005	allemand	anglais		2E
488820DE	JACQUEY	Marc	13/11/2005	anglais	italien		2D
024810CE	JULIANO	Alberto	21/04/2005	anglais	espagnol		2C
249992EJ	KLEIBER	Gusti	20/02/2005	anglais	espagnol	cinéma	2E
492698AF	LACOUR	Julie	06/04/2005	italien	anglais		2D
026454FA	LARBI	Nourdine	14/07/2005	espagnol	anglais		2C
309341GD	LEFZA	Yasmina	26/11/2005	espagnol	anglais		2E
076725HD	MARTIN	Victor	13/03/2005	anglais	espagnol		2A
815183CB	NGUYEN	Ngong	16/03/2005	anglais	espagnol		2D
094002FC	PELTIER	Romane	14/06/2005	allemand	anglais		2D
321262HD	RENAULT	Zoé	06/08/2005	anglais	espagnol	latin	2E
075421AK	ROTH	Ursule	03/01/2005	anglais	allemand		2A
121001CK	SERHANI	Sabrina	01/09/2005	italien	anglais		2D
538965DJ	TUDJANE	Yourk	31/01/2005	espagnol	anglais		2D
389873GC	VIALET	Priscille	28/02/2005	espagnol	anglais		2C
980306CA	WADE	Marcelin	03/05/2005	allemand	anglais		2E
807158DH	WENGER	Alexandre	20/08/2005	allemand	anglais		2A
666702FA	YAMAN	Elamine	23/04/2005	anglais	arabe		2D

figure 1: Extrait du fichier `seconde_lyc.csv`



Pour les besoins de l'organisation du lycée, le chef d'établissement exploite la base de données par des requêtes en langage SQL. Il a pour cela créé une table (ou relation) SQL dénommée seconde dans son système de gestion de bases de données dont la structure est la suivante :

seconde
num_eleve (clef primaire)
langue1
langue2
option
classe

L'attribut num_eleve est un entier, les autres sont des chaînes de caractère (le type CHAR).

Q5. Dans le modèle relationnel, **donner** l'intérêt de l'attribut num_eleve.

On suppose que la table seconde contient les informations issues de la figure 1 (ni plus, ni moins, même si la figure 1 n'est qu'un extrait du fichier seconde_lyc.csv).

Q6. Donner le résultat de la requête

SELECT num_eleve FROM seconde ;

On rappelle qu'en SQL, la fonction d'agrégation COUNT() permet de compter le nombre d'enregistrements dans une table.

Q7. Donner le résultat de la requête

SELECT COUNT(num_eleve) FROM seconde ;

Q8. Écrire la requête seconde permettant de connaître le nombre d'élèves qui font allemand en langue1 ou langue2.

Le chef d'établissement souhaite faire évoluer la structure de sa base de données. Pour ce faire, il crée une nouvelle table eleve dont la structure est la suivante :

eleve
num_eleve (clef primaire, clef étrangère de la table seconde)
nom
prenom
datenaissance

Là encore, l'attribut num_eleve est un entier, les autres sont des chaînes de caractère (le type CHAR).

Q9. Expliquer ce qu'apporte l'information clef étrangère pour l'attribut num_eleve de cette table en termes d'intégrité et de cohérence.

On suppose la table eleve correctement créée et complétée. Le chef d'établissement aimerait lister les élèves (nom, prénom, date de naissance) de la classe 2A.

Q10. Écrire la commande qui permet d'établir cette liste à l'aide d'une jointure entre eleve et seconde.

Q11. Proposer la structure d'une table coordonnees dans laquelle on pourra indiquer, pour chaque élève, son adresse, son code postal, sa ville, son adresse mail. **Préciser** la clef primaire et/ou la clé étrangère en vue de la mise en relation avec les autres tables.

