

Documents autorisés. Pas de calculettes. Pas d'ordinateur. Pas de téléphone.
IMPORTANT : Notez le numéro de sujet sur votre copie.
 Les étoiles marquent les exercices difficiles.

Question 1

Le but de cet exercice est d'appliquer l'algorithme de compression LZ78 à la chaîne de caractères « OLGOEEOEXXHHG ». On rappelle que l'algorithme démarre avec un dictionnaire contenant la seule association

$$\varepsilon \rightarrow 0$$

(où ε représente la chaîne vide), et remplit le dictionnaire avec les préfixes rencontrés au fur et à mesure qu'il parcourt la chaîne en entrée.

- Donner le dictionnaire de l'algorithme.
- Donner la liste des couples (préfixe, symbole) en sortie de l'algorithme.
- Mettre le dictionnaire sous forme d'arbre.
- On va coder les symboles sur 5 bits : A est codé par 00000, B par 00001, etc. Les préfixes sont codés en longueur variable, comme défini par l'algorithme LZ78. Donner la sortie binaire de l'algorithme.

Question 2

On reporte ici le tableau définissant UTF-8.

Code point	bits	Octet 1	Octet 2	Octet 3	Octet 4
U+0000 - U+007F	7	0xxxxxxx			
U+0080 - U+07FF	11	110xxxxx	10xxxxxx		
U+0800 - U+FFFF	16	1110xxxx	10xxxxxx	10xxxxxx	
U+10000 - U+1FFFFF	21	11110xxx	10xxxxxx	10xxxxxx	10xxxxxx

- Encodez le *code-point* Unicode U+b6e9.
- Décodez les octets suivants en une suite de *code-points*

0xcf 0x81 0xe5 0x80 0x8b 0xf0 0x94 0x95 0x94

Question 3

On veut transmettre un message sur un canal bruité. Pour cela, on commence par encoder les lettres de l'alphabet sur 5 bits par l'écriture en base 2 de leur position : A = 00001, B = 00010, etc.

- Encodez le message « BLEU »

Ensuite, pour permettre la correction d'erreurs, on découpe le message en blocs de 4 bits et on applique le code linéaire de paramètres [8, 4, 4] défini par la matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

- Calculez la matrice de parité du code.
- Combien d'erreurs au plus peut corriger ce code ?
- Encodez le message de la question (a).

- (e) Décodez le message « 10010001 10011110 11011010 10101110 01010010 ».
- (f) (*) Donnez un exemple de mot qui ne peut pas être décodé de façon unique. À l'aide de la matrice de parité, montrez que le mot ne peut pas être décodé.

Question 4

- (a) Combien vaut $7^{20} \pmod{33}$?
- (b) Quels sont les ordres possibles pour les éléments de $\mathbb{Z}/33\mathbb{Z}$?
- (c) Calculez $23^{13} \pmod{33}$.
- (d) Trouvez un élément de $\mathbb{Z}/33\mathbb{Z}$ d'ordre 2.

Question 5

On fixe le module RSA $N = 65$.

- (a) Calculez $\phi(N)$.
- (b) On fixe la clef publique $e = 37$. Calculez la clef privée.
- (c) (*) Décodez le message $c = 47$ à l'aide de la partie de la table de multiplication donnée en annexe. (**Suggestion** : pour faire les calculs, il sera commode de représenter les entiers modulaires entre 33 et 65 par leur représentant négatif).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	-31	-29	-27	-25	-23	-21	-19	-17	-15	-13	-11	-9	-7	-5	-3	-1
3	3	6	9	12	15	18	21	24	27	30	-32	-29	-26	-23	-20	-17	-14	-11	-8	-5	-2	1	4	7	10	13	16	19	22	25	28	31
4	4	8	12	16	20	24	28	32	-29	-25	-21	-17	-13	-9	-5	-1	3	7	11	15	19	23	27	31	-30	-26	-22	-18	-14	-10	-6	-2
5	5	10	15	20	25	30	-30	-25	-20	-15	-10	-5	0	5	10	15	20	25	30	-30	-25	-20	-15	-10	-5	0	5	10	15	20	25	30
6	6	12	18	24	30	-29	-23	-17	-11	-5	1	7	13	19	25	31	-28	-22	-16	-10	-4	2	8	14	20	26	32	-27	-21	-15	-9	-3
7	7	14	21	28	-30	-23	-16	-9	-2	5	12	19	26	-32	-25	-18	-11	-4	3	10	17	24	31	-27	-20	-13	-6	1	8	15	22	29
8	8	16	24	32	-25	-17	-9	-1	7	15	23	31	-26	-18	-10	-2	6	14	22	30	-27	-19	-11	-3	5	13	21	29	-28	-20	-12	-4
9	9	18	27	-29	-20	-11	-2	7	16	25	-31	-22	-13	-4	5	14	23	32	-24	-15	-6	3	12	21	30	-26	-17	-8	1	10	19	28
10	10	20	30	-25	-15	-5	5	15	25	-30	-20	-10	0	10	20	30	-25	-15	-5	5	15	25	-30	-20	-10	0	10	20	30	-25	-15	-5
11	11	22	-32	-21	-10	1	12	23	-31	-20	-9	2	13	24	-30	-19	-8	3	14	25	-29	-18	-7	4	15	26	-28	-17	-6	5	16	27
12	12	24	-29	-17	-5	7	19	31	-22	-10	2	14	26	-27	-15	-3	9	21	-32	-20	-8	4	16	28	-25	-13	-1	11	23	-30	-18	-6
13	13	26	-26	-13	0	13	26	-26	-13	0	13	26	-26	-13	0	13	26	-26	-13	0	13	26	-26	-13	0	13	26	-26	-13	0	13	26
14	14	28	-23	-9	5	19	-32	-18	-4	10	24	-27	-13	1	15	29	-22	-8	6	20	-31	-17	-3	11	25	-26	-12	2	16	30	-21	-7
15	15	30	-20	-5	10	25	-25	-10	5	20	-30	-15	0	15	30	-20	-5	10	25	-25	-10	5	20	-30	-15	0	15	30	-20	-5	10	25
16	16	32	-17	-1	15	31	-18	-2	14	30	-19	-3	13	29	-20	-4	12	28	-21	-5	11	27	-22	-6	10	26	-23	-7	9	25	-24	-8
17	17	-31	-14	3	20	-28	-11	6	23	-25	-8	9	26	-22	-5	12	29	-19	-2	15	32	-16	1	18	-30	-13	4	21	-27	-10	7	24
18	18	-29	-11	7	25	-22	-4	14	32	-15	3	21	-26	-8	10	28	-19	-1	17	-30	-12	6	24	-23	-5	13	31	-16	2	20	-27	-9
19	19	-27	-8	11	30	-16	3	22	-24	-5	14	-32	-13	6	25	-21	-2	17	-29	-10	9	28	-18	1	20	-26	-7	12	31	-15	4	23
20	20	-25	-5	15	-30	-10	10	30	-15	5	25	-20	0	20	-25	-5	15	-30	-10	10	30	-15	5	25	-20	0	20	-25	-5	15	-30	-10
21	21	-23	-2	19	-25	-4	17	-27	-6	15	-29	-8	13	-31	-10	11	32	-12	9	30	-14	7	28	-16	5	26	-18	3	24	-20	1	22
22	22	-21	1	23	-20	2	24	-19	3	25	-18	4	26	-17	5	27	-16	6	28	-15	7	29	-14	8	30	-13	9	31	-12	10	32	-11
23	23	-19	4	27	-15	8	31	-11	12	-30	-7	16	-26	-3	20	-22	1	24	-18	5	28	-14	9	32	-10	13	-29	-6	17	-25	-2	21
24	24	-17	7	31	-10	14	-27	-3	21	-20	4	28	-13	11	-30	-6	18	-23	1	25	-16	8	32	-9	15	-26	-2	22	-19	5	29	-12
25	25	-15	10	-30	-5	20	-20	5	30	-10	15	-25	0	25	-15	10	-30	-5	20	-20	5	30	-10	15	-25	0	25	-15	10	-30	-5	20
26	26	-13	13	-26	0	26	-13	13	-26	0	26	-13	13	-26	0	26	-13	13	-26	0	26	-13	13	-26	0	26	-13	13	-26	0	26	-13
27	27	-11	16	-22	5	32	-6	21	-17	10	-28	-1	26	-12	15	-23	4	31	-7	20	-18	9	-29	-2	25	-13	14	-24	3	30	-8	19
28	28	-9	19	-18	10	-27	1	29	-8	20	-17	11	-26	2	30	-7	21	-16	12	-25	3	31	-6	22	-15	13	-24	4	32	-5	23	-14
29	29	-7	22	-14	15	-21	8	-28	1	30	-6	23	-13	16	-20	9	-27	2	31	-5	24	-12	17	-19	10	-26	3	32	-4	25	-11	18
30	30	-5	25	-10	20	-15	15	-20	10	-25	5	-30	0	30	-5	25	-10	20	-15	15	-20	10	-25	5	-30	0	30	-5	25	-10	20	-15
31	31	-3	28	-6	25	-9	22	-12	19	-15	16	-18	13	-21	10	-24	7	-27	4	-30	1	32	-2	29	-5	26	-8	23	-11	20	-14	17
32	32	-1	31	-2	30	-3	29	-4	28	-5	27	-6	26	-7	25	-8	24	-9	23	-10	22	-11	21	-12	20	-13	19	-14	18	-15	17	-16

Quadrant supérieur de la table de multiplication de $\mathbb{Z}/65\mathbb{Z}$