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

(a) Construisez l'arbre d'un code de Huffman pour l'alphabet suivant, en tenant compte des fréquences d'apparition données :

A	B	C	D	E	F	G	H	I	J	K	L
7.7%	13.1%	10.0%	7.9%	2.4%	10.6%	3.0%	13.0%	5.2%	11.0%	6.8%	9.4%

(b) Encodez le mot « JILCF ».

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

1. Encodez le *code-point* Unicode `U+c2b6`.
2. Décodez les octets suivants en une suite de *code-points*

0xe8 0x98 0x8c 0xee 0x96 0x8d 0xf0 0x9e 0x8a 0x99

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.

(a) Encodez le message « PLUS »

Ensuite, pour permettre la correction d'erreurs, on applique lettre par lettre le code linéaire de paramètres $[9, 5, 3]$ défini par la matrice génératrice

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

(b) Calculez la matrice de parité du code.

(c) Combien d'erreurs au plus peut corriger ce code ?

(d) Encodez le message de la question (a).

(e) Décodez le message « 101101110 110101000 101011010 100111111 ».

(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) Quels sont les ordres possibles pour les éléments de $\mathbb{Z}/19\mathbb{Z}$?

(b) Calculez l'ordre de 12 mod 19.

(c) Calculez 12^{13} mod 19.

(d) Trouvez un élément de $\mathbb{Z}/19\mathbb{Z}$ d'ordre 3.

Question 5

On fixe le module RSA $N = 55$.

(a) Calculez $\phi(N)$.

(b) On fixe la clef publique $e = 7$. Calculez la clef privée.

(c) ($*$) Décodez le message $c = 2$ 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 28 et 55 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
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
2	2	4	6	8	10	12	14	16	18	20	22	24	26	-27	-25	-23	-21	-19	-17	-15	-13	-11	-9	-7	-5	-3	-1
3	3	6	9	12	15	18	21	24	27	-25	-22	-19	-16	-13	-10	-7	-4	-1	2	5	8	11	14	17	20	23	26
4	4	8	12	16	20	24	-27	-23	-19	-15	-11	-7	-3	1	5	9	13	17	21	25	-26	-22	-18	-14	-10	-6	-2
5	5	10	15	20	25	-25	-20	-15	-10	-5	0	5	10	15	20	25	-25	-20	-15	-10	-5	0	5	10	15	20	25
6	6	12	18	24	-25	-19	-13	-7	-1	5	11	17	23	-26	-20	-14	-8	-2	4	10	16	22	-27	-21	-15	-9	-3
7	7	14	21	-27	-20	-13	-6	1	8	15	22	-26	-19	-12	-5	2	9	16	23	-25	-18	-11	-4	3	10	17	24
8	8	16	24	-23	-15	-7	1	9	17	25	-22	-14	-6	2	10	18	26	-21	-13	-5	3	11	19	27	-20	-12	-4
9	9	18	27	-19	-10	-1	8	17	26	-20	-11	-2	7	16	25	-21	-12	-3	6	15	24	-22	-13	-4	5	14	23
10	10	20	-25	-15	-5	5	15	25	-20	-10	0	10	20	-25	-15	-5	5	15	25	-20	-10	0	10	20	-25	-15	-5
11	11	22	-22	-11	0	11	22	-22	-11	0	11	22	-22	-11	0	11	22	-22	-11	0	11	22	-22	-11	0	11	22
12	12	24	-19	-7	5	17	-26	-14	-2	10	22	-21	-9	3	15	27	-16	-4	8	20	-23	-11	1	13	25	-18	-6
13	13	26	-16	-3	10	23	-19	-6	7	20	-22	-9	4	17	-25	-12	1	14	27	-15	-2	11	24	-18	-5	8	21
14	14	-27	-13	1	15	-26	-12	2	16	-25	-11	3	17	-24	-10	4	18	-23	-9	5	19	-22	-8	6	20	-21	-7
15	15	-25	-10	5	20	-20	-5	10	25	-15	0	15	-25	-10	5	20	-20	-5	10	25	-15	0	15	-25	-10	5	20
16	16	-23	-7	9	25	-14	2	18	-21	-5	11	27	-12	4	20	-19	-3	13	-26	-10	6	22	-17	-1	15	-24	-8
17	17	-21	-4	13	-25	-8	9	26	-12	5	22	-16	1	18	-20	-3	14	-24	-7	10	27	-11	6	23	-15	2	19
18	18	-19	-1	17	-20	-2	16	-21	-3	15	-22	-4	14	-23	-5	13	-24	-6	12	-25	-7	11	-26	-8	10	-27	-9
19	19	-17	2	21	-15	4	23	-13	6	25	-11	8	27	-9	10	-26	-7	12	-24	-5	14	-22	-3	16	-20	-1	18
20	20	-15	5	25	-10	10	-25	-5	15	-20	0	20	-15	5	25	-10	10	-25	-5	15	-20	0	20	-15	5	25	-10
21	21	-13	8	-26	-5	16	-18	3	24	-10	11	-23	-2	19	-15	6	27	-7	14	-20	1	22	-12	9	-25	-4	17
22	22	-11	11	-22	0	22	-11	11	-22	0	22	-11	11	-22	0	22	-11	11	-22	0	22	-11	11	-22	0	22	-11
23	23	-9	14	-18	5	-27	-4	19	-13	10	-22	1	24	-8	15	-17	6	-26	-3	20	-12	11	-21	2	25	-7	16
24	24	-7	17	-14	10	-21	3	27	-4	20	-11	13	-18	6	-25	-1	23	-8	16	-15	9	-22	2	26	-5	19	-12
25	25	-5	20	-10	15	-15	10	-20	5	-25	0	25	-5	20	-10	15	-15	10	-20	5	-25	0	25	-5	20	-10	15
26	26	-3	23	-6	20	-9	17	-12	14	-15	11	-18	8	-21	5	-24	2	-27	-1	25	-4	22	-7	19	-10	16	-13
27	27	-1	26	-2	25	-3	24	-4	23	-5	22	-6	21	-7	20	-8	19	-9	18	-10	17	-11	16	-12	15	-13	14

Quadrant supérieur de la table de multiplication de $\mathbb{Z}/55\mathbb{Z}$

Solutions

Solution 1 Trop fatiguant à générer automatiquement. Voir cours.

Solution 2

(a) Le code-point `U+c2b6` est compris entre `U+0800` et `U+FFFF`, il va donc être encodé sur 3 octets. L'écriture binaire du code-point est

$$1100001010110110.$$

D'après le tableau, le premier octet est obtenu en concaténant 1110 avec les 4 bits de poids fort du code-point (éventuellement en ajoutant des 0 à gauche pour que le code-point fasse 16 bits) , ce qui donne

$$11101100,$$

ou en hexadécimal 0xec. Les deux octets suivants sont obtenus en concaténant 10 avec les deux blocs de 6 bits restants. Cela donne 0x8a et 0xb6. En conclusion, l'encodage utf-8 du code-point `U+c2b6` est

$$0\text{xec } 0\text{x8a } 0\text{xb6}.$$

(b) Pour une lecture plus facile, on commence par réécrire en binaire le flux de données :

11101000 10011000 10001100 11101110 10010110 10001101 11110000 10011110 10001010 10011001

Grâce au tableau d'encodage, on peut découper ce flux en trois caractères Unicode :

$$\begin{aligned}&11101000\ 10011000\ 10001100,\\&11101110\ 10010110\ 10001101,\\&11110000\ 10011110\ 10001010\ 10011001.\end{aligned}$$

Toujours à l'aide du tableau d'encodage, on déduit les trois code-points suivants (en binaire)

$$1000011000001100\ 1110010110001101\ 11110001010011001,$$

ou, en hexadécimal

$$\text{U+860c U+e58d U+1e299}.$$

Solution 3

(a) En appliquant lettre par lettre le codage, on a

$$10000\ 01100\ 10101\ 10011.$$

(b) La matrice de parité du code est

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

(c) La distance minimale du code est 3, donc le code peut corriger au plus $(3-1)/2 = 1$ erreur.

(d) Pour encoder le message précédent, il suffit de le multiplier lettre par lettre par la matrice G. Cela donne

$$100000011\ 011000011\ 101011001\ 100111111.$$

(e) On commence par calculer les quatre syndromes en multipliant chaque mot par la matrice H, cela nous donne

$$1011, \quad 1110, \quad 0011, \quad 0000.$$

En cherchant l'indice auquel les syndromes apparaissent dans H, on obtient les pattern d'erreur suivants

$$000100000\ 010000000\ 100000000\ 000000000,$$

qui, additionnés aux mots reçus, donnent les mots de code

$$101001110\ 100101000\ 001011010\ 100111111.$$

Il ne reste plus qu'à trouver le message correspondant à chaque mot de code, ce qui se lit dans les cinq premières coordonnées :

$$10100\ 10010\ 00101\ 10011.$$

Enfin, en inversant le codage du premier point, on obtient le message « TRES ».

Solution 4

(a) Par le petit théorème de Fermat, l'ordre des éléments de $\mathbb{Z}/19\mathbb{Z}$ divise 18.

(b) On vérifie par un calcul direct que l'ordre de 12 mod 19 est 6.

(c) Par conséquent, $12^{13} = 12$.

(d) Un élément qui a nécessairement ordre 3 est $12^2 = 11$.

Solution 5

(a) On a $\phi(N) = \phi(5 \cdot 11) = (5-1) \cdot (11-1) = 40$.

(b) La clef privée d est l'inverse de e modulo $\phi(N)$. En utilisant l'algorithme d'Euclide étendu, on obtient la relation

$$3\phi(N) + (-17)e = 3 \cdot 40 + (-17) \cdot 7 = 1.$$

On en déduit

$$-17e = 23e = 1 \mod \phi(N)$$

et donc $d = 23$.

(c) Sur la diagonale de la table de multiplication, on trouve les carrés successifs de 2 modulo 55 :

$$(2)^2 = (4), \quad (4)^2 = (16), \quad (16)^2 = (-19), \quad (-19)^2 = (-24), \quad (-24)^2 = (26).$$

En utilisant l'algorithme d'exponentiation binaire :

$$2^{23} = 2 \cdot 4 \cdot 16 \cdot 31 = 8,$$