Question 1

On considère l'alphabet formé des symboles suivants, avec leurs fréquences d'apparition :

F	S	C	D	N	R	M	H	L	A	K	U
1%	1%	2%	3%	3%	5%	7%	11%	12%	12%	13%	30%

(a) Construisez l'arbre d'un code de Huffman pour cet alphabet.

(b) Encodez le message « HUFFMAN ».

Question 2

On considère le chiffrement par permutation avec pour clef la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$$

(a) Encodez le message « TOUSNIERTOUSNIERAUTO ».

(b) Décodez le message « NCEAMMAEASOUBRSUPOTL ».

(c) On a vu en cours que le chiffrement par permutation est un cas particulier du chiffrement de Hill. Donnez les matrices d'encodage et décodage qui correspondent à la clef ci-dessus.

Question 3

Voici la matrice génératrice d'un code linéaire 1-correcteur de paramètres $[7, 3, 4]$

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

(a) Écrivez sa matrice de parité.

(b) Encodez les messages suivants : 010, 000, 101.

(c) En utilisant le *décodage par syndrome*, décodez les messages suivants 0010111, 1010111, 0111101.

(d) Le mot 1100000 n'est à distance 1 d'aucun mot du code. Il est à distance 2 du mot de code 0000000, mais, puisque la distance minimale du code est 4, il se pourrait que ce décodage ne soit pas unique. Trouvez un autre mot de code qui se trouve à distance 2 de 1100000 (**Suggestion :** calculez le syndrome de 1100000, puis trouvez un autre mot de poids 2 ayant le même syndrome).

Question 4

(a) Calculez le pgcd de 91 et 119. 91 est-il inversible modulo 119 ?

(b) Calculez l'inverse de 19 modulo 28. Calculez 19^6 modulo 28.

Question 5

Alice et Bob veulent convenir d'un secret en utilisant le protocole d'échange de clef de Diffie-Hellman. Ils se mettent d'accord pour le corps $\mathbb{Z}/11\mathbb{Z}$ et pour le générateur $g = 7$. Alice choisit la clef secrète $a = 8$ et Bob $b = 9$.

(a) Calculez les clefs publiques de Alice et Bob.

(b) Calculez la clef partagée.

Utilisez l'algorithme d'exponentiation binaire pour répondre aux deux questions. Ne donnez pas seulement les résultats finaux : développez en détail les étapes du calcul.

(c) Calculez 5^{402} mod 11.

Question 6

On choisit le module RSA $N = 35 = 5 * 7$, et la clef publique $e = 7$. La table de multiplication de $\mathbb{Z}/35\mathbb{Z}$ est donnée en annexe.

(a) Calculez la clef privée du cryptosystème.

(b) Encodez l'entier 3 avec la clef publique à l'aide de l'algorithme d'exponentiation binaire.

(c) Décodez le résultat et vérifiez la cohérence de vos calculs.

	0	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	33	34
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	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	33	34
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
3	0	3	6	9	12	15	18	21	24	27	30	33	1	4	7	10	13	16	19	22	25	28	31	34	2	5	8	11	14	17	20	23	26	29	32
4	0	4	8	12	16	20	24	28	32	1	5	9	13	17	21	25	29	33	2	6	10	14	18	22	26	30	34	3	7	11	15	19	23	27	31
5	0	5	10	15	20	25	30	0	5	10	15	20	25	30	0	5	10	15	20	25	30	0	5	10	15	20	25	30	0	5	10	15	20	25	30
6	0	6	12	18	24	30	1	7	13	19	25	31	2	8	14	20	26	32	3	9	15	21	27	33	4	10	16	22	28	34	5	11	17	23	29
7	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28
8	0	8	16	24	32	5	13	21	29	2	10	18	26	34	7	15	23	31	4	12	20	28	1	9	17	25	33	6	14	22	30	3	11	19	27
9	0	9	18	27	1	10	19	28	2	11	20	29	3	12	21	30	4	13	22	31	5	14	23	32	6	15	24	33	7	16	25	34	8	17	26
10	0	10	20	30	5	15	25	0	10	20	30	5	15	25	0	10	20	30	5	15	25	0	10	20	30	5	15	25	0	10	20	30	5	15	25
11	0	11	22	33	9	20	31	7	18	29	5	16	27	3	14	25	1	12	23	34	10	21	32	8	19	30	6	17	28	4	15	26	2	13	24
12	0	12	24	1	13	25	2	14	26	3	15	27	4	16	28	5	17	29	6	18	30	7	19	31	8	20	32	9	21	33	10	22	34	11	23
13	0	13	26	4	17	30	8	21	34	12	25	3	16	29	7	20	33	11	24	2	15	28	6	19	32	10	23	1	14	27	5	18	31	9	22
14	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21
15	0	15	30	10	25	5	20	0	15	30	10	25	5	20	0	15	30	10	25	5	20	0	15	30	10	25	5	20	0	15	30	10	25	5	20
16	0	16	32	13	29	10	26	7	23	4	20	1	17	33	14	30	11	27	8	24	5	21	2	18	34	15	31	12	28	9	25	6	22	3	19
17	0	17	34	16	33	15	32	14	31	13	30	12	29	11	28	10	27	9	26	8	25	7	24	6	23	5	22	4	21	3	20	2	19	1	18
18	0	18	1	19	2	20	3	21	4	22	5	23	6	24	7	25	8	26	9	27	10	28	11	29	12	30	13	31	14	32	15	33	16	34	17
19	0	19	3	22	6	25	9	28	12	31	15	34	18	2	21	5	24	8	27	11	30	14	33	17	1	20	4	23	7	26	10	29	13	32	16
20	0	20	5	25	10	30	15	0	20	5	25	10	30	15	0	20	5	25	10	30	15	0	20	5	25	10	30	15	0	20	5	25	10	30	15
21	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14
22	0	22	9	31	18	5	27	14	1	23	10	32	19	6	28	15	2	24	11	33	20	7	29	16	3	25	12	34	21	8	30	17	4	26	13
23	0	23	11	34	22	10	33	21	9	32	20	8	31	19	7	30	18	6	29	17	5	28	16	4	27	15	3	26	14	2	25	13	1	24	12
24	0	24	13	2	26	15	4	28	17	6	30	19	8	32	21	10	34	23	12	1	25	14	3	27	16	5	29	18	7	31	20	9	33	22	11
25	0	25	15	5	30	20	10	0	25	15	5	30	20	10	0	25	15	5	30	20	10	0	25	15	5	30	20	10	0	25	15	5	30	20	10
26	0	26	17	8	34	25	16	7	33	24	15	6	32	23	14	5	31	22	13	4	30	21	12	3	29	20	11	2	28	19	10	1	27	18	9
27	0	27	19	11	3	30	22	14	6	33	25	17	9	1	28	20	12	4	31	23	15	7	34	26	18	10	2	29	21	13	5	32	24	16	8
28	0	28	21	14	7	0	28	21	14	7	0	28	21	14	7	0	28	21	14	7	0	28	21	14	7	0	28	21	14	7	0	28	21	14	7
29	0	29	23	17	11	5	34	28	22	16	10	4	33	27	21	15	9	3	32	26	20	14	8	2	31	25	19	13	7	1	30	24	18	12	6
30	0	30	25	20	15	10	5	0	30	25	20	15	10	5	0	30	25	20	15	10	5	0	30	25	20	15	10	5	0	30	25	20	15	10	5
31	0	31	27	23	19	15	11	7	3	34	30	26	22	18	14	10	6	2	33	29	25	21	17	13	9	5	1	32	28	24	20	16	12	8	4
32	0	32	29	26	23	20	17	14	11	8	5	2	34	31	28	25	22	19	16	13	10	7	4	1	33	30	27	24	21	18	15	12	9	6	3
33	0	33	31	29	27	25	23	21	19	17	15	13	11	9	7	5	3	1	34	32	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2
34	0	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

TABLE 1 – Table de multiplication de $\mathbb{Z}/35\mathbb{Z}$.