MAT 2450

Quatrième série d'exercices

Exercice A. Alain, Béatrice et Catherine sont associés dans une compagnie. Pour communiquer entre eux ils utilisent des codes RSA. Pour simplifier ils ont tous pris la même clé n. Béatrice demande d'utiliser une clé d'encryption e_B et Catherine une clé d'encryption e_C. Il se trouve que $(e_B, e_C) = 1$. Alain doit envoyer une information confidentielle m à Béatrice et Catherine et on a $(m, n) = 1$. Alain encode donc l'information pour Béatrice dans le message m'_B et pour Catherine dans le message m'_C. Un espion capte les deux messages encodés m'_B et m'_C. Expliquer comment il peut facilement retrouver le message m confidentiel. Ceci signifie qu'une telle pratique n'est pas sécuritaire.

Exercice B. Voici un principe simple de cryptographie. Le carré blanc □ est représenté par le chiffre 0. Les lettres $A, \ldots, Z$ par les nombres $1, \ldots, 26$. Le nombre 27 correspond au point et le nombre 28, à la virgule. La table ci-dessous résume ceci :

Symbole à coder	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Nombre associé	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Symbole à coder	P	Q	R	S	T	U	V	W	X	Y	Z	.	,
Nombre associé	16	17	18	19	20	21	22	23	24	25	26	27	28

Voici comment on code un mot :

- on remplace les symboles par leurs nombres associés ;
- pour chaque symbole, on calcule le reste de la division par 29 de 3^n, où n est le nombre associé au symbole ;
- on réduit le résultat obtenu modulo 29 ;
- on trouve les symboles correspondant aux nombres obtenus : ceci nous donne le mot codé.

Par exemple, pour coder le mot « DE » on remplace ses lettres par les nombres $4, 5$. On calcule $3^4, 3^5$ et on obtient $81, 243$. On les réduit modulo 29, ce qui donne $23, 11$. La lettre associée à 23 est W ; celle associée à 11 est K. Le mot codé représentant « DE » est « WK ».

(a) Coder le mot « JET ».

(b) Expliquer pourquoi le code est inversible, c'est-à-dire pourquoi les lettres de code sont toutes distinctes.

(c) Décoder le mot « XMF ».