Thème : Quelques applications des congruences

Corrigé de l'activité 7.

Exercice 1 : *Chiffrement de Hill*

Voir le fichier tableur pf5372b07.chiffrement_de_hill_tableur.xls ou pf5372b07.chiffrement_de_hill_tableur.ods

Partie A *Chiffrement*

1) On fait le tableau des rangs n des 26 lettres de l'alphabet :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang n	0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- La matrice $U = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ contient les rangs du couple de lettres en clair $(C; D)$.

  Posons $V = A \times U$

$$\begin{pmatrix} 3 & 5 \\ 6 & 11 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad \begin{pmatrix} 3\times 2 + 5 \times 3 \\ 6 \times 2 + 11 \times 3 \end{pmatrix}$$

$$A \times \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 21 \\ 45 \end{pmatrix} \qquad V = \begin{pmatrix} 21 \\ 45 \end{pmatrix}$$

  Le reste de la division de $p_1 = 21$ par 26 est $n'_1 = 21$.

  Le reste de la division de $p_2 = 45$ par 26 est $n'_2 = 19$.

  Donc $W = \begin{pmatrix} 21 \\ 19 \end{pmatrix}$. W contient les rangs du couple de lettres chiffrées $(V; T)$.

  Ainsi, le mot "CD" est chiffré en "**VT**".

2) Chiffrement avec la même clé du mot « AX »

- La matrice $U = \begin{pmatrix} 0 \\ 23 \end{pmatrix}$ contient les rangs du couple de lettres en clair $(A; X)$.

  Posons $V = A \times U$

  On obtient à la calculatrice $V = \begin{pmatrix} 115 \\ 253 \end{pmatrix}$.

  Le reste de la division de $p_1 = 115$ par 26 est $n'_1 = 11$.

  Le reste de la division de $p_2 = 253$ par 26 est $n'_2 = 19$.

  Donc $W = \begin{pmatrix} 11 \\ 19 \end{pmatrix}$. W contient les rangs du couple de lettres chiffrées $(L; T)$.

  Ainsi, le mot "AX" est chiffré en "**LT**".

3) Avec les exemples précédents, on voit que pour deux mots en clair aux lettres toutes distinctes, obtient dans les deux mots chiffrés la lettre T plusieurs fois.
Donc deux lettres distinctes ne sont pas chiffrées en deux lettres distinctes.

4) On réalise le tableau suivant avec un tableur : Voir le fichier chiffrement_de_hill_tableur

	A	B	C	D	E
1	Clé	$a11=$	3	$a12=$	5
2		$a21=$	6	$a22=$	11
3	Couples de Lettres en clair	N	M	R	
4		O	B	E	
5	Rang $n1$	13	12	17	####
6	Rang $n2$	14	1	4	####
7	$p1$	109	41	71	####
8	$p2$	232	83	146	####
9	Rang $n'1$	5	15	19	####
10	Rang $n'2$	24	5	16	####
11	Couples de lettres chiffrées	**F**	**P**	**T**	####
12		**Y**	**F**	**Q**	####

- La cellule B5 contient la formule =CODE(B3)-65
  La cellule B6 contient la formule =CODE(B4)-65
- La cellule B7 contient la formule =$C1*B$5+$E1*B$6
  La cellule B8 contient la formule =$C2*B$5+$E2*B$6

} Formules du produit matriciel $A \times U$.
Le $ permet de fixer la référence de la colonne ou de la ligne lors de la recopie automatique.

- La cellule B9 contient la formule =MOD(B7;26)
  La cellule B10 contient la formule = MOD(B8;26)
- La cellule B11 contient la formule =CAR(B9+65)
  La cellule B12 contient la formule = CAR(B10+65)

Le mot « NOMBRE » est chiffré en « **FYPFTQ** ».

Partie B *Déchiffrement*

1) Par lecture de la table de codage de la question 1) de la partie A, on a :

$$W_1 = \begin{pmatrix} 5 \\ 24 \end{pmatrix}, \quad W_2 = \begin{pmatrix} 15 \\ 5 \end{pmatrix}, \quad W_3 = \begin{pmatrix} 19 \\ 16 \end{pmatrix}.$$

2) a) On a :

$$C \times A = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$$

b) On a :
$C \times A = 3I_2$ avec $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Donc $\frac{1}{3}C \times A = I_2$. Donc la matrice A est inversible.

c) La matrice inverse de A est $A^{-1} = \frac{1}{3}C$.

$$A^{-1} = \begin{pmatrix} \frac{11}{3} & -\frac{5}{3} \\ -2 & 1 \end{pmatrix}$$

d) A la calculatrice, on obtient :

$$A^{-1} \times W_1 = \begin{pmatrix} -\frac{65}{3} \\ 14 \end{pmatrix} \qquad A^{-1} \times W_2 = \begin{pmatrix} \frac{140}{3} \\ -25 \end{pmatrix} \qquad A^{-1} \times W_3 = \begin{pmatrix} 43 \\ -22 \end{pmatrix}$$

e) La clé A^{-1} donne des matrices à coefficients parfois non entiers. Elle ne permet donc pas le déchiffrement.

3) On effectue les produit matriciels :

$$9C \times W_1 = \begin{pmatrix} -585 \\ 378 \end{pmatrix} \qquad 9C \times W_2 = \begin{pmatrix} 1260 \\ -675 \end{pmatrix} \qquad 9C \times W_3 = \begin{pmatrix} 1161 \\ -594 \end{pmatrix}$$

$-585 \equiv 13 \ \ (26)$ $378 \equiv 14 \ \ (26)$	$\begin{pmatrix} 13 \\ 14 \end{pmatrix}$	contient les rangs du couple de lettres en clair $(N; O)$.
$1260 \equiv 12 \ \ (26)$ $-675 \equiv 1 \ \ (26)$	$\begin{pmatrix} 12 \\ 1 \end{pmatrix}$	contient les rangs du couple de lettres en clair $(M; B)$.
$1161 \equiv 17 \ \ (26)$ $-594 \equiv 4 \ \ (26)$	$\begin{pmatrix} 17 \\ 4 \end{pmatrix}$	contient les rangs du couple de lettres en clair $(R; E)$.

La clé $9C$ permet donc le déchiffrement du message « **FYPFTQ** »

Remarque :

On peut se demander d'où vient la matrice C.
$C = \det(A) \times A^{-1}$ donc C est la comatrice transposée de A, c'est à dire $C = {}^t com(A)$
Dans l'exemple, $\det(A) = 3$. Le coefficient 9 est l'inverse de 3 modulo 26 ce qui permet de simplifier les relations de congruence.
De façon générale, toute matrice A dont le déterminant est premier avec 26 convient comme clé de chiffrement puisque dans ce cas $\det(A)$ a un inverse modulo 26.

4) • Considérons le chiffrement d'un couple de lettres en clair quelconques, de rangs $(n_1; n_2)$. n_1 et n_2 sont des entiers appartenant à $E = \{0; 1; 2; 3; \dots; 25\}$. Considérons la clé de chiffrement $A = \begin{pmatrix} 3 & 5 \\ 6 & 11 \end{pmatrix}$.

On définit la matrice $U_1 = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$.

- Pour chiffrer, on calcule la matrice

$V_1 = A \times U_1 \qquad V_1 = \begin{pmatrix} 3n_1 + 5n_2 \\ 6n_1 + 11n_2 \end{pmatrix}$

- Pour trouver les rangs des lettres du couple chiffré, on calcule la matrice

$W_1 = \begin{pmatrix} n_1' \equiv 3n_1 + 5n_2 \ \ (26) \\ n_2' \equiv 6n_1 + 11n_2 \ \ (26) \end{pmatrix}$ où n_1' et n_2' sont des entiers appartenant à $E = \{0; 1; 2; 3; \dots; 25\}$.

• Considérons le déchiffrement du couple de lettres chiffrées de rangs $(n_1'; n_2')$ avec la clé de déchiffrement $9C$ où $C = \begin{pmatrix} 11 & -5 \\ -6 & 3 \end{pmatrix}$

On a $W_1 = \begin{pmatrix} n_1' \\ n_2' \end{pmatrix}$.

- Pour déchiffrer, on calcule la matrice

$9C \times W_1 = 9\begin{pmatrix} 11 & -5 \\ -6 & 3 \end{pmatrix} \times \begin{pmatrix} n_1' \\ n_2' \end{pmatrix}$

$$9C \times W_1 = 9\begin{pmatrix} 11n_1' - 5n_2' \\ -6n_1' + 3n_2' \end{pmatrix}$$

$$9C \times W_1 = \begin{pmatrix} 9 \times (11n_1' - 5n_2') \\ 9 \times (-6n_1' + 3n_2') \end{pmatrix}$$

- Montrons que cette matrice permet de toujours obtenir les rangs n_1 et n_2 du couple de lettres en clair.

Or, de par la méthode de chiffrement, on a $\begin{cases} n_1' \equiv 3n_1 + 5n_2 \quad (26) \\ n_2' \equiv 6n_1 + 11n_2 \quad (26) \end{cases}$

Donc, les facteurs qui apparaissent dans la matrice $9C \times W_1$ vérifient

$$\begin{cases} 11n_1' - 5n_2' \equiv 11(3n_1 + 5n_2) - 5(6n_1 + 11n_2) \quad (26) \\ -6n_1' + 3n_2' \equiv -6(3n_1 + 5n_2) + 3(6n_1 + 11n_2) \quad (26) \end{cases}$$

$$\begin{cases} 11n_1' - 5n_2' \equiv 3n_1 \quad (26) \\ -6n_1' + 3n_2' \equiv 3n_2 \quad (26) \end{cases}$$

On retrouve les éléments de la matrice $9C \times W_1$ en multipliant les deux membres par 9 (qui est l'inverse de 3 modulo 26) :

$$\begin{cases} 9 \times (11n_1' - 5n_2') \equiv 27n_1 \quad (26) \\ 9 \times (-6n_1' + 3n_2') \equiv 27n_2 \quad (26) \end{cases}$$

Et comme $27 \equiv 1 \quad (26)$

$$\begin{cases} 9 \times (11n_1' - 5n_2') \equiv n_1 \quad (26) \\ 9 \times (-6n_1' + 3n_2') \equiv n_2 \quad (26) \end{cases}$$

Ainsi :

$9C \times W_1 = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$ où n_1 et n_2 sont des entiers appartenant à $E = \{0; 1; 2; 3; \dots; 25\}$.

Conclusion :

La clé $9C$ avec $C = 3A^{-1} = \begin{pmatrix} 11 & -5 \\ -6 & 3 \end{pmatrix}$ et $9C = 27A^{-1} = \begin{pmatrix} 99 & -45 \\ -54 & 27 \end{pmatrix}$ permet de déchiffrer tous les messages chiffrés avec la clé $A = \begin{pmatrix} 3 & 5 \\ 6 & 11 \end{pmatrix}$.

5) Déchiffrement du message « **MPYORQZL** »

- La matrice $W_1 = \begin{pmatrix} 12 \\ 15 \end{pmatrix}$ contient les rangs du couple de lettres $(\boldsymbol{M}; \boldsymbol{P})$

On déchiffre ce couple en faisant le produit $9C \times W_1$.

On obtient à la calculatrice $9C \times W_1 = \begin{pmatrix} 513 \\ -243 \end{pmatrix}$.

$\begin{cases} 513 \equiv 19 \quad (26) \\ -243 \equiv 17 \quad (26) \end{cases}$ donc $\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{pmatrix} 19 \\ 17 \end{pmatrix}$

$\begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$ contient les rangs du couple de lettres en clair $(T; R)$.

- La matrice $W_2 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$ contient les rangs du couple de lettres $(\boldsymbol{Y}; \boldsymbol{O})$

On déchiffre ce couple en faisant le produit $9C \times W_2$.

On obtient à la calculatrice $9C \times W_2 = \begin{pmatrix} 1746 \\ -918 \end{pmatrix}$.

$\begin{cases} 1746 \equiv 4 \ \ (26) \\ -918 \equiv 18 \ \ (26) \end{cases}$ donc $\begin{pmatrix} n_3 \\ n_4 \end{pmatrix} = \begin{pmatrix} 4 \\ 18 \end{pmatrix}$

$\begin{pmatrix} n_3 \\ n_4 \end{pmatrix}$ contient les rangs du couple de lettres en clair $(E; S)$.

- La matrice $W_3 = \begin{pmatrix} 17 \\ 16 \end{pmatrix}$ contient les rangs du couple de lettres $(\boldsymbol{R}; \boldsymbol{Q})$

On déchiffre ce couple en faisant le produit $9C \times W_3$.

On obtient à la calculatrice $9C \times W_3 = \begin{pmatrix} 963 \\ -486 \end{pmatrix}$.

$\begin{cases} 963 \equiv 1 \ \ (26) \\ -486 \equiv 8 \ \ (26) \end{cases}$ donc $\begin{pmatrix} n_5 \\ n_6 \end{pmatrix} = \begin{pmatrix} 1 \\ 8 \end{pmatrix}$

$\begin{pmatrix} n_5 \\ n_6 \end{pmatrix}$ contient les rangs du couple de lettres en clair $(B; I)$.

- La matrice $W_4 = \begin{pmatrix} 25 \\ 11 \end{pmatrix}$ contient les rangs du couple de lettres $(\boldsymbol{Z}; \boldsymbol{L})$

On déchiffre ce couple en faisant le produit $9C \times W_4$.

On obtient à la calculatrice $9C \times W_4 = \begin{pmatrix} 1980 \\ -1053 \end{pmatrix}$.

$\begin{cases} 1980 \equiv 4 \ \ (26) \\ -1053 \equiv 13 \ \ (26) \end{cases}$ donc $\begin{pmatrix} n_7 \\ n_8 \end{pmatrix} = \begin{pmatrix} 4 \\ 13 \end{pmatrix}$

$\begin{pmatrix} n_7 \\ n_8 \end{pmatrix}$ contient les rangs du couple de lettres en clair $(E; N)$.

Ainsi le message déchiffré est « TRESBIEN ».

Exercice 2 : *Chiffrement RSA*

Partie A : Alice décide de choisir (*n* ; *e*) = (21 ; 5) comme clé publique.

1) a) Elle peut effectivement faire ce choix, en effet :
- 21 est égal au produit de deux nombres premiers : $21 = 3 \times 7$. On a $p = 3 \quad q = 7$.
- On a alors $m = (3-1)(7-1) = 12$ et $e = 5$ est premier avec 12 et 5 est compris entre 1 et 12.

b) Le choix de $n = 21$ ne permet pas d'assurer la sécurité du message. Il est en effet beaucoup trop simple de factoriser n et donc de déterminer une clé privée.

2) a) On a $p = 3 \quad q = 7 \quad m = 12$.

b) $5d \equiv 1 \ (12) \ \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $5d = 12k + 1$.

Or $5d = 12k + 1 \ \Leftrightarrow \ 5d - 12k = 1$

5 et 12 sont premiers entre eux donc d'après le théorème de Bézout, l'équation (*E*) admet des solutions.

c) Soit par essais successifs, soit en utilisant la calculatrice, soit en utilisant l'algorithme d'Euclide, on peut trouver : $d = 5$, $k = 2$ comme solution particulière de l'équation $5d - 12k = 1$.

d) Résolution de l'équation : $5d - 12k = 1$.

$$\begin{array}{lll} 5 \times d & -12 \times k & = 1 \\ 5 \times 5 & -12 \times 2 & = 1 \\ \hline 5(d-5) - 12(k-2) = 0 & \Leftrightarrow & 5(d-5) = 12(k-2) \end{array}$$

Or 5 et 12 sont premiers entre eux et 5 divise $12(k-2)$ donc d'après le théorème de Gauss, 5 divise $(k-2)$ donc il existe un entier α tel que $k - 2 = 5\alpha$ et donc il existe un entier α tel que $k = 5\alpha + 2$.
De plus, $5d - 12k = 1$; on a alors $5d = 1 + 12k = 1 + 12(5\alpha + 2) = 60\alpha + 25$.
On a donc $d = 12\alpha + 5$.
Les solutions de l'équation (*E*) sont donc les entiers d appartenant à $\{12\alpha + 5 \ ; \ \alpha \in \mathbb{Z}\}$.

e) Parmi les clés privées proposées, la seule possible est donc (21 ; 17). Alice a choisi $\alpha = 1$. Elle utilisera par la suite cette clé pour déchiffrer les messages de Bob.

3) a) En associant à chaque lettre du mot PAL, sa place dans l'alphabet, on trouve :

$$M_1 = 16 \quad M_2 = 1 \quad M_3 = 12.$$

b) Par définition, $0 \leq C_1 < 21$ et $C_1 \equiv 16^5 \ (21) \ \Leftrightarrow \ 16^5 \equiv C_1 \ (21)$. Donc $C_1 = 4$.

De même, on a $C_2 = 1 \quad C_3 = 3$.

c) Le message chiffré envoyé par Bob : 4 1 3.

4) a) La clé privée de déchiffrement est (21 ; 17).

On sait que $M_1 \equiv 4^{17} \ (21)$ avec $0 \leq M_1 < n$. Donc $M_1 = 16$. On a de même $M_2 = 1$, $M_3 = 12$.

b) En associant les lettres correspondantes, le message envoyé par Bob était donc PAL.

Partie B : Alice a choisi (55 ; 3) comme clé privée.

1) Dans Liste3, ce sont les restes de la division par 55 des entiers de Liste1 élevés à la puissance 3 qui sont calculés.

2) La séquence de touches pour obtenir les trois listes est la suivante :

Sur calculatrice TI (TI 82 – 83)	Sur calculatrice Casio (GRAPH 35+ USB)
• Appuyer sur la touche Stats Dans le menu EDIT, choisir 4: EffListe Effacer les listes L_1, L_2, L_3 précédentes en saisissant EffListe L_1,L_2,L_3 entrée • Appuyer sur la touche Stats Dans le menu EDIT, choisir 1: EDIT • Amener le curseur sur le titre de la colonne L_1 entrée 2nd Listes , OP, 5: suite entrée Saisir suite(X,X,1,54,1) entrée La colonne L_1 se remplit des entiers de 1 à 54. • Amener le curseur sur le titre de la colonne L_2 entrée Dans la zone en bas, à gauche de L_2=, taper la formule L_1^3 entrée La colonne L_2 se remplit des cubes des éléments de L_1 • Amener le curseur sur le titre de la colonne L_3 entrée Dans la zone en bas, à gauche de L_3=, taper la formule L_2 – 55*partEnt(L_2/55) entrée La colonne L_3 se remplit des restes de la division des éléments de L_2 par 55.	• Aller dans le menu **STAT** Effacer les List 1 List 2 List 3 précédentes en mettant en surbrillance un élément de ces listes. Appuyer sur F6, aller dans DEL-A (touche F4) et valider "Yes". Amener le curseur sur le Titre de la première Liste List 1 • Aller dans le menu **RUN-MAT** • Appuyer sur la touche OPTN Aller dans LIST (touche F1) puis Seq (touche F5) Saisir Seq(X,X,1,54,1) → List 1 puis appuyer sur EXE SHIFT QUIT • Appuyer sur la touche OPTN Aller dans LIST (touche F1) puis (puis List (touche F1) Saisir (List 1)^3 → List 2 puis appuyer sur EXE SHIFT QUIT • Appuyer sur la touche OPTN Aller dans LIST (touche F1) puis (puis List (touche F1) Saisir (List 2) − 55×Intg((List 2)÷55) → List 3 puis appuyer sur EXE SHIFT QUIT • Aller dans le menu **STAT** Vérifier que les List 1 List 2 List 3 sont correctement remplies.

On obtient :

Liste 1 (Codes chiffrés C_i)	Liste 2 (calcul intermédiaire)	Liste3 (Codes en clair M_i)
1	1	**1**
2	8	8
3	27	27
4	64	9
5	125	**15**
6	216	51
…	…	…

3) Le tableau précédent permet donc à Alice de déchiffrer le message reçu.

A chaque valeur C_i codant le message chiffré (*C*) qui a été envoyé par Bob, le tableau permet d'associer la valeur M_i codant la lettre en clair à lire dans la troisième colonne.

(*C*) code chiffré	10	**1**	7	25	24	18	**5**	9	49
(*M*) code en clair	10	**1**	13	5	19	2	**15**	14	4
Lettre en clair	**J**	**A**	**M**	**E**	**S**	**B**	**O**	**N**	**D**

Partie C : Alice a choisi (221 ; 35) comme clé privée.

1) Dans Liste3, ce sont les restes de la division par 221 des entiers de Liste1 élevés à la puissance 35.
La séquence de touches pour obtenir les trois listes est la suivante :

Sur calculatrice TI (TI 82 – 83)	Sur calculatrice Casio (GRAPH 35+ USB)
• Appuyer sur la touche Stats Dans le menu EDIT, choisir 4: EffListe Effacer les listes L_1, L_2, L_3 précédentes en saisissant EffListe L_1,L_2,L_3 entrée • Appuyer sur la touche Stats Dans le menu EDIT, choisir 1: EDIT • Amener le curseur sur le titre de la colonne L_1 entrée 2nd Listes , OP, 5: suite entrée Saisir suite(X,X,1,220,1) entrée La colonne L_1 se remplit des entiers de 1 à 220. • Amener le curseur sur le titre de la colonne L_2 entrée Dans la zone en bas, à droite de L_2=, taper la formule L_1^35 entrée La colonne L_2 se remplit des puissances 35 des éléments de L_1 • Amener le curseur sur le titre de la colonne L_3 entrée Dans la zone en bas, à droite de L_3=, taper la formule $L_2 - 221$*partEnt(L_2/221) entrée La colonne L_3 se remplit des restes de la division des éléments de L_2 par 221.	• Aller dans le menu **STAT** Effacer les List 1 List 2 List 3 précédentes en mettant en surbrillance un élément de ces listes. Appuyer sur F6, aller dans DEL-A (touche F4) et valider "Yes". Amener le curseur sur le Titre de la première Liste List 1 • Aller dans le menu **RUN-MAT** • Appuyer sur la touche OPTN Aller dans LIST (touche F1) puis Seq (touche F5) Saisir Seq(X,X,1,220,1) → List 1 puis appuyer sur EXE SHIFT QUIT • Appuyer sur la touche OPTN Aller dans LIST (touche F1) puis (puis List (touche F1) Saisir (List 1)^35 → List 2 puis appuyer sur EXE SHIFT QUIT • Appuyer sur la touche OPTN Aller dans LIST (touche F1) puis (puis List (touche F1) Saisir (List 2) − 221×Intg((List 2)÷221) → List 3 puis appuyer sur EXE SHIFT QUIT • Aller dans le menu **STAT** Vérifier que les List 1 List 2 List 3 sont correctement remplies.

On obtient :

Liste 1 (Codes chiffrés C_i)	Liste 2 (calcul intermédiaire)	Liste3 (Codes en clair M_i)
1	1	1
2	$3.4^{E}10$	59
3	**$5^{E}16$**	**0**
4	$1.2^{E}21$	0
5	$2.9^{E}24$	0
6	$1.7^{E}27$	0
…	…	…

Les valeurs dans la troisième liste peuvent être nulles à cause d'un dépassement de la taille des nombres que la calculatrice est capable de stocker. Dans ce cas, l'affichage de la liste 3 ne permet pas de déchiffrer.

Soit $C_i = 3$.	3^{35} (calcul intermédiaire)	Le reste dans la division de 3^{35} par 221 (Code en clair M_i)
Affichage calculatrice	$5{,}00315450 \times 10^{16}$	0 - valeur fausse -
Valeur exacte	50031545098999707	61 - valeur correcte -

Pour calculer le reste d'une division euclidienne, il est impératif de ne travailler qu'avec des valeurs exactes !
Or la calculatrice ne permet pas de le faire au-delà de nombres entiers de plus de 13 chiffres.

2) a) On sait que pour tout entier naturel C, $C \equiv C \ \ (221)$ et donc si $C^{n-1} \equiv R \ \ (221)$ alors d'après la compatibilité des congruences et de la multiplication, on a $C^{n-1} \times C \equiv R \times C \ \ (221)$

Donc, si $C^{n-1} \equiv R \ \ (221)$ alors $C^n \equiv R \times C \ \ (221)$.

b) L'algorithme complété :

ENTREE :
C entier naturel

TRAITEMENT ET SORTIE :
Saisir $\boldsymbol{C}$
R prend la valeur **1**
Pour *I* allant de 1 à **35**
    $\boldsymbol{R}$ prend la valeur $R \times C - 221 \times \text{partEnt}(R \times C/221)$
Fin Pour
Afficher $\boldsymbol{R}$

3) Le programme sur la calculatrice :

Programme PUISSANC sur TI

```
Prompt C
1→R
For(I,1,35)
R*C−221*PartEnt(R*C/221)→R
End
Disp R
```

Programme PUISSANC sur Casio

```
"C="?→C
1→R
For 1→I To 35
R×C−221×Intg(R×C/221)→R
Next
R◢
ClrText
```

En utilisant ce programme Alice associe à chaque valeur C_i du message (*C*) envoyé la valeur M_i affichée. Elle obtient :

C_i	126	164	208	164	76	76	1	184	164	27	164	76	1
M_i	3	5	13	5	19	19	1	7	5	14	5	19	1
(*M*) en clair	C	E	M	E	S	S	A	G	E	N	E	S	A

200	41	111	166	164	41	86	200	185	86	1	152	1	76
21	20	15	4	5	20	18	21	9	18	1	16	1	19
U	T	O	D	E	T	R	U	I	R	A	P	A	S