Thème : Quelques applications des congruences

Corrigé de l'activité 3. Déchiffrement affine

Exercice 1

1) On fait le tableau des codes x des 26 lettres de l'alphabet :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Code	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 lettre en clair G a pour code $x = 6$
  $17x + 22 = 124$.
  Le reste de la division de 124 par 26 est $y = 20$
  Donc G est chiffré par U.
- La lettre en clair R a pour code $x = 17$
  $17x + 22 = 311$.
  Le reste de la division de 311 par 26 est $y = 25$
  Donc R est chiffré par Z.
- La lettre en clair I a pour code $x = 8$
  $17x + 22 = 158$
  Le reste de la division de 158 par 26 est $y = 2$
  Donc I est chiffré par C.
- La lettre en clair S a pour code $x = 18$
  $17x + 22 = 328$.
  Le reste de la division de 328 par 26 est $y = 16$
  Donc S est chiffré par Q.

Ainsi GRIS est chiffré en UZCQ.

2) Soit un entier u tel que $17u \equiv 1 \quad (26)$
   a) Si $17u \equiv 1 \quad (26)$ alors il existe un entier k tel que $17u - 1 = 26k$ or $26k$ est pair donc $17u$ est impair et donc u est impair.

   b) On procède par essais successifs des premiers entiers impairs :

u	1	3	5	7	9	11	13	15	17	19	21	23
$17u$	17	51	85	119	153	187	221	255	289	323	357	391
$17u \equiv \cdots \quad (26)$	17	25	7	15	23	5	13	21	3	11	19	**1**

D'après ces essais, $u = 23$.

3) On suit la méthode indiquée :

$$y \equiv 17x + 22 \quad (26)$$

$$y - 22 \equiv 17x \quad (26)$$

$$17x \equiv y - 22 \quad (26)$$

$$23 \times 17x \equiv 23 \times (y - 22) \quad (26)$$

Or, $23 \times 17 \equiv 1 \quad (26)$ donc :

$$x \equiv 23 \times (y - 22) \quad (26)$$

$$x \equiv 23y - 506 \quad (26)$$

et en simplifiant, puisque $506 \equiv 12 \quad (26)$, on a :

$$x \equiv 23y - 12 \quad (26)$$

4) On utilise la fonction de déchiffrement :

- La lettre chiffrée S a pour code $y = 18$
  $23y - 12 = 402$.
  Le reste de la division de 402 par 26 est $x = 12$
  Donc la lettre en clair est M.
- La lettre chiffrée W a pour code $y = 22$
  $23y - 12 = 494$.
  Le reste de la division de 494 par 26 est $x = 0$
  Donc la lettre en clair est A.
- La lettre chiffrée Z a pour code $y = 25$
  $23y - 12 = 563$.
  Le reste de la division de 563 par 26 est $x = 17$
  Donc la lettre en clair est R.
- La lettre chiffrée Q a pour code $y = 16$
  $23y - 12 = 356$.
  Le reste de la division de 356 par 26 est $x = 18$
  Donc la lettre en clair est S.

Donc SWZQ est déchiffré en MARS.

Exercice 2

Partie A

1)

c	a	b
0		
	25	
		7
1		
	18	
2		
	11	
3		
	4	

L'algorithme affiche $c = 3$ et $a = 4$.

2) L'algorithme affiche le quotient c et le reste a de la division de a par b.

Partie B

1) La lettre en clair L a pour code $m = 11$

$3m + 5 = 38$.
Le reste de la division de 38 par 26 est $p = 12$
Donc L est chiffré par M.

2) Algorithme :

Déclaration des variables

a, m, p sont des entiers
Commentaire : p est le reste de la division de $3m + 5$ par 26

Début de l'algorithme

Saisir m
a prend la valeur $3m + 5$
Tant que $a \geq 26$
    Affecter à a la valeur $a - 26$
Fin Tant que
Afficher "$p =$ " , a

Fin de l'algorithme

Partie C

1) $x = 9$ est une solution de $3x \equiv 1 \ \ (26)$

* $3m + 5 \equiv p \ \ (26)$

implique successivement

* $9(3m + 5) \equiv 9p \ \ (26)$
* $27m + 45 \equiv 9p \ \ (26)$
* $m \equiv 9p - 45 \ \ (26)$
* $m \equiv 9p + 7 \ \ (26)$

Réciproquement :

* $m \equiv 9p + 7 \ \ (26)$

implique successivement

* $3m \equiv 3(9p + 7) \ \ (26)$
* $3m \equiv 27p + 21 \ \ (26)$
* $3m - 21 \equiv p \ \ (26)$
* $p \equiv 3m + 5 \ \ (26)$

Conclusion :

Les propositions $3m + 5 \equiv p \ \ (26)$ et $m \equiv 9p + 7 \ \ (26)$ sont équivalentes.

2) Déchiffrement de la lettre M :

- La lettre chiffrée M a pour code $p = 12$
  $9p + 7 = 115$.
  Le reste de la division de 115 par 26 est $m = 11$
  Donc la lettre en clair est L.

Partie D

Clé	a=	9		b=	7														
Lettre chiffrée	**M**	**R**	**H**		**H**	**F**	**S**	**X**	**M**	**V**	**K**	**H**		**M**	**V**	**S**	**X**	**H**	
Rang p	12	17	7		7	5	18	23	12	21	10	7		12	21	18	23	7	
$ap + b$	115	160	70		70	52	169	214	115	196	97	70		115	196	169	214	70	
Rang m	11	4	18		18	0	13	6	11	14	19	18		11	14	13	6	18	
Lettre en clair	L	E	S		S	A	N	G	L	O	T	S		L	O	N	G	S	

O	**R**	**H**		**Q**	**D**	**V**	**M**	**V**	**S**	**H**		**O**	**R**		**M**		**F**	**N**	**K**	**V**	**P**	**S**	**R**
14	17	7		16	3	21	12	21	18	7		14	17		12		5	13	10	21	15	18	17
133	160	70		151	34	196	115	196	169	70		133	160		115		52	124	97	196	142	169	160
3	4	18		21	8	14	11	14	13	18		3	4		11		0	20	19	14	12	13	4
D	E	S		V	I	O	L	O	N	S		D	E		L		A	U	T	O	M	N	E