

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 $17u \equiv 1 \pmod{26}$

- a) Si $17u \equiv 1 \pmod{26}$ 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
$17u \equiv \dots \pmod{26}$	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.