**7.7**

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 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 transcription numérique de SOS est 18 14 18.

Pour coder le S, il faut calculer $18^{17} \mod 3233$ :

| $x$ | reste $r$ | $n$ | $18^{2^n} \mod 3233$ | contribution (si $r = 1$) |
|---|---|---|---|---|
| 17 | 1 | 0 | 18 | 18 |
| 8 | 0 | 1 | $18^2 \equiv 324$ | |
| 4 | 0 | 2 | $324^2 \equiv 1520$ | |
| 2 | 0 | 3 | $1520^2 \equiv -1195$ | |
| 1 | 1 | 4 | $(-1195)^2 \equiv -961$ | $-961$ |

$18^{17} \equiv 18 \cdot (-961) \equiv 2100 \mod 3233$
Le S est donc crypté en 2100.

Pour coder le O, il faut calculer $14^{17} \mod 3233$ :

| $x$ | reste $r$ | $n$ | $14^{2^n} \mod 3233$ | contribution (si $r = 1$) |
|---|---|---|---|---|
| 17 | 1 | 0 | 14 | 14 |
| 8 | 0 | 1 | $14^2 \equiv 196$ | |
| 4 | 0 | 2 | $196^2 \equiv -380$ | |
| 2 | 0 | 3 | $(-380)^2 \equiv -1085$ | |
| 1 | 1 | 4 | $(-1085)^2 \equiv 413$ | 413 |

$14^{17} \equiv 14 \cdot 413 \equiv 2549 \mod 3233$
Le O est ainsi crypté en 2549.

On envoie par conséquent le message crypté 2100 2549 2100.

Pour procéder au déchiffrement du message, il faut déterminer la clé de décryptage $d$. On a $n = 3233 = 53 \cdot 61$ et $\varphi(n) = (53-1)(61-1) = 3120$.
Résolvons l'équation diophantienne $17\,x + 3120\,y = 1$ :

$$\begin{aligned} 3120 &= 17 \cdot 183 + 9 && \Longrightarrow && 9 = 3120 - 17 \cdot 183 \\ 17 &= 9 \cdot 1 + 8 && \Longrightarrow && 8 = 17 - 9 \cdot 1 \\ 9 &= 8 \cdot 1 + 1 && \Longrightarrow && 1 = 9 - 8 \cdot 1 \\ 8 &= 1 \cdot 8 \end{aligned}$$

$$\begin{aligned} 1 &= 9 - 8 \cdot 1 \\ &= 9 - (17 - 9 \cdot 1) \cdot 1 = 17 \cdot (-1) + 9 \cdot 2 \\ &= 17 \cdot (-1) + (3120 - 17 \cdot 183) \cdot 2 = 3120 \cdot 2 + 17 \cdot (-367) \end{aligned}$$

À partir de la solution particulière $x_0 = -367$ et $y_0 = 2$, on déduit la solution générale :

$$\begin{cases} x = -367 + \frac{3120}{1}\,k = -367 + 3120\,k \\ y = \quad 2 - \frac{17}{1}\,k = \quad 2 - \quad 17\,k \end{cases} \quad \text{où } k \in \mathbb{Z}$$

La condition $1 < x < \varphi(n) = 3120$ implique $k = 1$.
On conclut que $d = -367 + 3120 = 2753$.

Pour décoder le nombre 2100, il faut calculer $2100^{2753} \mod 3233$ :

| $x$ | reste $r$ | $n$ | $2100^{2^n} \mod 3233$ | contribution (si $r = 1$) |
|---|---|---|---|---|
| 2753 | 1 | 0 | 2100 | 2100 |
| 1376 | 0 | 1 | $2100^2 \equiv 188$ | |
| 688 | 0 | 2 | $188^2 \equiv -219$ | |
| 344 | 0 | 3 | $(-219)^2 \equiv -534$ | |
| 172 | 0 | 4 | $(-534)^2 \equiv 652$ | |
| 86 | 0 | 5 | $652^2 \equiv 1581$ | |
| 43 | 1 | $61581^2 \equiv 452$ | 452 | |
| 21 | 1 | 7 | $452^2 \equiv 625$ | 625 |
| 10 | 0 | 8 | $625^2 \equiv -568$ | |
| 5 | 1 | 9 | $(-568)^2 \equiv -676$ | $-676$ |
| 2 | 0 | 10 | $(-676)^2 \equiv 1123$ | |
| 1 | 1 | 11 | $1123^2 \equiv 259$ | 259 |

$2100^{2753} \equiv 2100 \cdot 452 \cdot 625 \cdot (-676) \cdot 259 \equiv 18 \mod 3233$
Le nombre 2100 est donc bien décodé en 18.

Pour décoder le nombre 2549, il faut calculer $2549^{2753} \mod 3233$ :

| $x$ | reste $r$ | $n$ | $2549^{2^n} \mod 3233$ | contribution (si $r = 1$) |
|---|---|---|---|---|
| 2753 | 1 | 0 | 2549 | 2549 |
| 1376 | 0 | 1 | $2549^2 \equiv -929$ | |
| 688 | 0 | 2 | $(-929)^2 \equiv -170$ | |
| 344 | 0 | 3 | $(-170)^2 \equiv -197$ | |
| 172 | 0 | 4 | $(-197)^2 \equiv 13$ | |
| 86 | 0 | 5 | $13^2 \equiv 169$ | |
| 43 | 1 | $6169^2 \equiv -536$ | $-536$ | |
| 21 | 1 | 7 | $(-536)^2 \equiv -441$ | $-441$ |
| 10 | 0 | 8 | $(-441)^2 \equiv 501$ | |
| 5 | 1 | 9 | $501^2 \equiv -1173$ | $-1173$ |
| 2 | 0 | 10 | $(-1173)^2 \equiv -1329$ | |
| 1 | 1 | 11 | $(-1329)^2 \equiv 1023$ | 1023 |

$2549^{2753} \equiv 2549 \cdot (-536) \cdot (-441) \cdot (-1173) \cdot 1023 \equiv 14 \mod 3233$
Le nombre 2549 est donc bien décodé en 14.

On a bien vérifié que le message codé 2100 2549 2100 était décodé en 18 14 18, ce qui correspond à la séquence des lettres SOS.