README pour le programme codageExponentiation
Ce programme consiste à coder/décoder des petits ou grand nombre
Voici un résumé du cryptage par exponentiation :

3.7 Codage par exponentiation

3.7.1 Le petit théorème de Fermat

THÉORÈME 3.7.1
Soit $\mathcal{P}$ l'ensemble des nombres premiers, et $p \in \mathcal{P}$:
- $\forall x \in \mathbb{N} : x^p \equiv x\,[p]$
- $\forall x \in \mathbb{N} : \mathbf{pgcd}(x,p) = 1 \Longrightarrow x^{p-1} \equiv 1\,[p]$

DÉMONSTRATION 3.7.1
Écrivons la formule du binôme de Newton :

$$(x+1)^p = x^p + C_p^1 x^{p-1} + \ldots + C_p^{p-1} x + 1$$

$\forall 1 \leq k \leq p-1 : k!C_p^k = p(p-1)(p-2)\ldots(p-k+1)$, mais p est premier, donc premier avec $k!$
En appliquant le théorème de Gauss, p divise C_p^k. Ainsi, en passant aux congruences :

$$(x+1)^p \equiv x^p + 1\,[p]$$

On peut alors démontrer le résultat par récurrence :
- Pour $x = 1$, $2^p \equiv 2\,[p]$
- Si $x^p \equiv x\,[p]$, alors $(x+1)^p \equiv x^p + 1\,[p] \equiv p+1\,[p]$, ce qui démontre la forme 1 du théorème.

Si x est premier avec p, on peut simplifier la congruence par x, ce qui donne la forme 2 du théorème.

3.7.2 Algorithme de codage

DÉFINITION 3.7.1
Soit p un nombre premier. On considère un nombre e premier avec $p-1$
- *La fonction de codage est définie de $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ par :*

$$f(x) \equiv x^e\,[p]$$

- *Le couple $(p.e)$ constitue la clé de codage.*

EXEMPLES 3.7.1
Codons le message "texte clair", après avoir effectué des regroupements de deux lettres, qui sont convertis en nombres compris entre 0000 et 2525. On doit donc choisir une valeur de p supérieure à 2525. Soit $p = 2633$ et $e = 29$. On vérifie que $\mathrm{pgcd}(29, 2632) = 1$. On utilise l'exponentiation rapide :

La décomposition de 29 en base 2 donne : $29 = 2^4 + 2^3 + 2^2 + 2^0$

[29/2]	29	14	7	3	1
Restes	1	0	1	1	1
k	0	1	2	3	4
1904^{2^k} [2633]	1904	2208	1581	844	1426
	1904	–	705	2595	1105

Cette opération effectuée pour chaque bloc, on obtient le message codé :

Caractère clair	t_i	te	xt	ec	la	ir
Chiffre clair	x_i	1904	2319	0402	1100	0817
Chiffre codé	$x_i^{29}\,[2633]$	1105	1185	2268	2261	2430

3.7.3 Algorithme de décodage

Les entiers e et $p-1$ sont premiers entre eux, donc il existe deux entiers d et k, obtenus par l'algorithme d'**Euclide** étendu tels que : $ed = 1 + k(p-1)$, c'est-à-dire : $ed \equiv 1\,[p-1]$
Rappelons que d est l'inverse de e modulo $p-1$
Alors $f(x)^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{1+k(p-1)} \equiv xx^{k(p-1)}\,[p]$
p est premier, et $\forall x : x < p$, donc x est premier avec p
D'après le petit théorème de **Fermat**, $x^{p-1} \equiv 1\,[p]$, donc $f(x)^d \equiv x\,[p]$
Donc la fonction de décodage est $x \equiv f^{-1}(y) \equiv y^d\,[p]$
La clé de décodage est le couple (p, d) où d est l'inverse de e modulo $p-1$

EXEMPLES 3.7.2
L'algorithme d'Euclide étendu donne $4 \times 2632 - 363 \times 29 = 1$
Alors, $d \equiv -363 + 2632 \equiv 2269\,[2632]$

Et on retrouve le texte clair : $1105^{2269} \equiv 1904\,[2633]$ par le tableau :

[2269/2]	2269	1134	567	283	141	70	35	17	8	4	2	1
Restes	1	0	1	1	1	0	1	1	0	0	0	1
k	0	1	2	3	4	5	6	7	8	9	10	11
1105^{2^k}	1105	1946	662	1166	928	193	387	2321	2556	663	2491	1733
	1105	–	2169	1374	700	–	2334	1133	–	–	–	1904

Ce type de codage résiste bien au décryptage si p est grand et si on effectue des regroupements d'au moins 4 caractères.

En résumé, on va prendre 2 voire 4 lettres et on va les coder. Par exemple prenons « ke », si on prend le nombre correspondant à l'emplacement de la lettre dans l'alphabet nous avons ceci : 1105 comme sur le tableau ci-dessus. Ce mode de codage consiste à coder un nombre avec une très grande puissance (ici c'est 2269) dans une grande base aussi (qui doit être supérieur au nombre à coder). On va donc décomposer la puissance dans la base 2. Et pour finir on va avoir le résultat qui est 1904 dans ce cas-là donc « ke » est codé en « sd ».