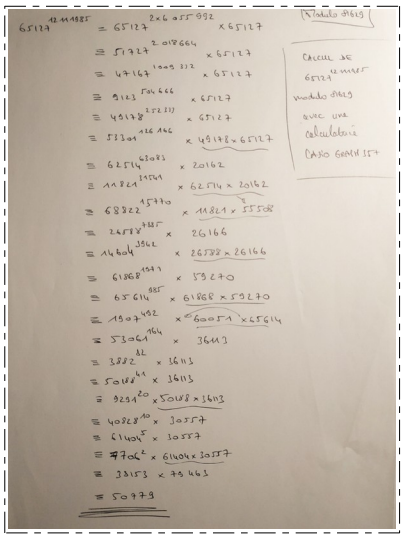
UN CHIFFREMENT À CLÉ PUBLIQUE :
LE PROTOCOLE D'ÉCHANGE DE CLÉS DE DIFFIE ET HELLMAN (1976)
CORRECTION

	Alice	Bob
Étape 1	Alice et Bob choisissent un nombre premier p et un entier a tel que $1 \leqslant a \leqslant p-1$. L'échange n'est pas sécurisé.	
Étape 2	Alice choisit secrètement un nombre x_1.	Bob choisit secrètement un nombre x_2.
Étape 3	Alice calcule y_1 tel que : $y_1 \equiv a^{x_1}[p]$.	Bob calcule y_2 tel que : $y_2 \equiv a^{x_2}[p]$.
Étape 4	Alice et Bob s'échangent les valeurs de y_1 et y_2. L'échange n'est pas sécurisé.	
Étape 5	Alice calcule la clé secrète $y_2^{x_1}[p]$	Bob calcule la clé secrète $y_1^{x_2}[p]$.

1. $y_2^{x_1} \equiv (a^{x_2})^{x_1}[p] \equiv a^{x_2 x_1}[p]$ et $y_1^{x_2} \equiv (a^{x_1})^{x_2}[p] \equiv a^{x_2 x_1}[p]$ d'où $y_2^{x_1} \equiv y_1^{x_2}[p]$.

2. On souhaite appliquer ce protocole avec les clés suivantes :
- clés publiques : $p = 81\,629$ et $a = 65\,127$.
- clés privées : $x_1 = 12\,111\,985$ et $x_2 = 29\,051\,994$.

a) Pour calculer à la main $y_1 \equiv 65127^{12\,111\,985}\,[81629]$, on pourrait utiliser la calculatrice en écrivant que $65127^2 \equiv 1660$ et en décomposant 12 111 985 en $2 \times 6\,055\,992 + 1$ et en recommençant à chaque fois…
C'est long => plus de 25 étapes :



b) Une méthode plus rapide existe, il s'agit de ***l'exponentiation modulaire rapide*** *(déjà vue)*.
La fonction Python `pow(a, e, n)` permet de calculer avec cette méthode a^e modulo n.
On trouve $y_1 = 50\,779$ et $y_2 = 38\,444$.
La clé secrète K est donc : $38\,444^{12\,111\,985}[p]$ ou $50\,779^{29\,051\,994}[p]$ *ie* 56 159.