Kid-RSA
L'algorithme Kid-RSA est un algorithme à but pédagogique proposé par Neal Koblitz.

Alice choisit quatre nombres *a*, *b*, *a1*, *b1*, puis calcule :

$$M = a \times b - 1$$
$$e = a1 \times M + a$$
$$d = b1 \times M + b$$
$$n = (e \times d - 1)/M$$

La clé publique d'Alice est (*n*, *e*) et sa clé privée est *d*.

Un message est sous la forme d'un nombre entier *P* strictement inférieur à *n*.
Le message codé *C* est le reste de la division euclidienne de $e \times P$ par *n*.
À partir du message codé *C*, on retrouve le message d'origine *P* en prenant le reste de la division euclidienne de $C \times d$ par *n*.

On prend *a* = 12, *b* = 16, *a1* = 7, *b1* = 20.

1. **a.** Déterminer la clé publique et la clé privée.

b. Coder le message *P* = 18 245.

c. Décoder le message *C* = 4 664.