Compter les clés dans le cadre du chiffre de Vigenère.

Objectif principal :	pratiquer les méthodes de dénombrement.
Objectifs secondaires :	comprendre un énoncé et le mettre en pratique, amorcer la discussion autour du chiffre de Vigenère ou des générateurs de clés aléatoires.

Précautions :	le chiffre de Vigenère n'est plus utilisé. Les **arrangements** apparaissent. On a besoin du **logarithme** pour la question **6**. Sans doute utile de faire une séance avant sur le chiffre de Vigenère ?

Proposition d'énoncé d'un exercice :

Le chiffre de Vigenère est une méthode utilisée du dix-septième au début du vingtième siècle pour chiffrer certains messages. Pour chiffrer et déchiffrer un message on choisit un mot, c'est-à-dire une suite de lettres sans signes de ponctuation ni espacements, de la taille de son choix. Ce mot est appelé la clé. A chaque clé différente correspond une façon de chiffrer et de déchiffrer différente.

1. Compter le nombre de clés de 5 lettres.

2. Compter le nombre de clés de 5 lettres dont toutes les lettres sont différentes.

3. Compter le nombre de clés de 5 lettres qui contiennent exactement deux *a*.

4. Compter le nombre de clés de 5 lettres qui contiennent au moins un *a*.

5. On cherche à d'obtenir des clés de dix lettres de la façon la plus aléatoire possible. On demande à une personne qui a l'habitude d'utiliser un ordinateur de taper dix lettres au hasard. Malheureusement, cette personne personne frappe alternativement des mains gauche et droite, et commence toujours par la gauche. Elle atteint 13 lettres de chacune des deux mains. Calculer le rapport du nombre de clés pouvant être ainsi obtenues par le nombre de clés qu'on espérait obtenir. Que penser de cette méthode ?

6. *Une autre faille.* On crypte des messages en changeant la clé de n lettres chaque jour. Lorsqu'on change la clé, on change systématiquement chacune des lettres (en se disant qu'une personne qui connaît la clé un jour ne pourra bénéficier d'un avantage le lendemain). On s'interdit donc d'utiliser chaque jour un certain nombre de clés. Calculer le nombre de lettres à partir duquel on perd plus de la moitié des clés disponibles.