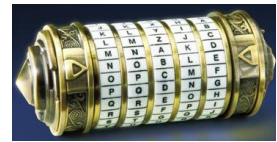


### Exercice n°1 : (2015)

Dans le « Da Vinci Code », Dan Brown fait utiliser cet objet (voir ci-contre).  
C'est une sorte de coffre-fort portable, capable de contenir des messages.



L'idée originale proviendrait de Léonard de Vinci.

Ce cryptex fonctionne comme un antivol de vélo. C'est un mot de cinq lettres qui actionnera la serrure et permettra d'ouvrir le cylindre. Ce cylindre contient un papier où a été inscrit un message.

Ce papier est enroulé autour d'un tube en verre fin contenant un produit chimique, ce qui empêche toute ouverture de force du cryptex pour obtenir le message : cela briserait le tube de verre et répandrait le produit chimique sur le papier qui deviendrait dès lors illisible.

Le cryptex est composé de cinq rouleaux, chacun comportant toutes les lettres de l'alphabet dans l'ordre usuel.

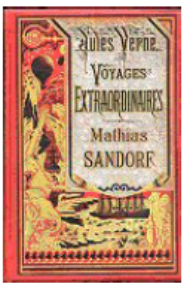
Ils sont tous sur la position donnant AAAAA au départ.

Pour découvrir le code et ouvrir le cryptex, John teste toutes les combinaisons en actionnant les rouleaux de la façon suivante :

la 1<sup>e</sup> combinaison testée est AAAAA, la 2<sup>e</sup> AAAAB, la 3<sup>e</sup> AAAAC, etc. Ainsi, la 26<sup>e</sup> combinaison testée est AAAAZ, puis la 27<sup>e</sup> AAABA, la 28<sup>e</sup> AAABB, la 29<sup>e</sup> AAABC, etc.

John met en moyenne 2 secondes pour tester chaque combinaison. Combien de temps (jours, heures, minutes et secondes) lui faudra-t-il pour ouvrir cet objet sachant que le mot permettant l'ouverture est E U L E R ?

### Exercice n°2 : (2014)

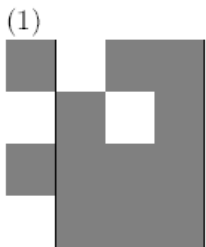
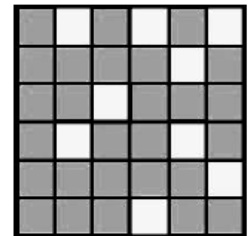


Après avoir lu le roman Mathias Sandorf de Jules Verne, Maxence et Sarah décident d'utiliser le même système de codage que celui évoqué dans le livre pour s'écrire des messages secrets.

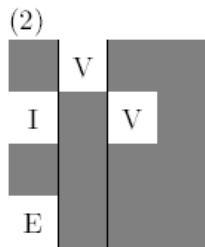
Le principe de ce codage est le suivant : on utilise un cache secret et une grille  $4 \times 4$ ,  $5 \times 5$ ,  $6 \times 6$  ... selon la longueur du message. Le cache, de même dimension que la grille, possède des trous, comme celui du roman de Jules Verne (voir ci-contre).

Sur l'exemple ci-dessous on illustre comment le message

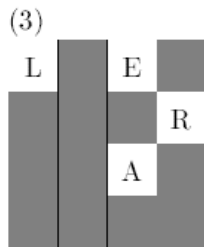
« VIVE LE RALLYE MATH » est codé en « LVEL IMVR ALAY ETEH ».



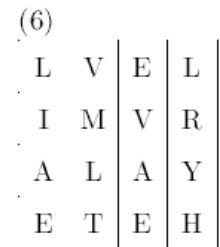
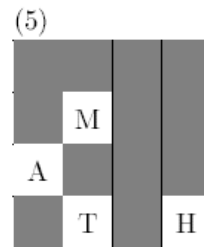
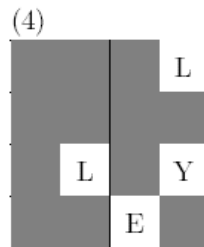
(1) Position initiale d'un cache  $4 \times 4$  sur une grille vide.



(2) On écrit les premières lettres du message dans les cases vides.

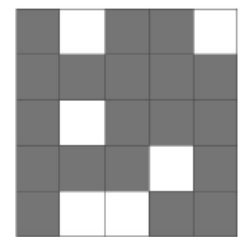


(3) Puis on fait tourner le cache d'un quart de tour dans le sens des aiguilles d'une montre. On continue de remplir le message. (4) On refait tourner le cache et on continue d'écrire. (5) On tourne de nouveau le cache et on finit d'écrire le message.

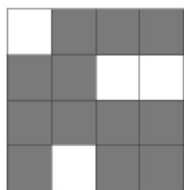


(6) On enlève le cache et on obtient le message codé.

- Afin de convenir d'un rendez-vous avec Sarah, Maxence désire coder le message suivant « A QUEL ENDROIT SE RENCONTRER ? » à l'aide de son cache  $5 \times 5$  représenté ci-contre dans sa position initiale.



Quel message va-t-il envoyer à Sarah ? (Il place le ? au centre du carré)

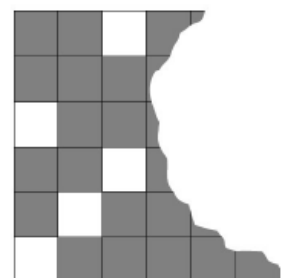


2.

Sarah lui renvoie le message suivant « RTUR EEDV CHSA UPDA ».

Quel message va décrypter Maxence à l'aide de son cache  $4 \times 4$  représenté ci-contre dans sa position initiale ?

- Pour écrire des messages plus longs, Maxence utilise un cache  $6 \times 6$  possédant 9 trous, cache qu'il a malheureusement abîmé. Voici le morceau restant représenté dans sa position initiale.



Reconstituer le cache.

### Exercice n°3 : (2016)

Le codage Playfair, a été popularisé par Lyon Playfair, mais il a été inventé par Sir Charles Wheatstone, un des pionniers du télégraphe électrique. Ce codage nécessite une grille 5×5 contenant 25 lettres. Pour la créer, on utilise les 26 lettres de l'alphabet auxquelles on enlève le W et on place les 25 lettres restantes dans un ordre que l'on choisit dans une grille 5×5 vierge. Pour le codage, on remplace les W du texte par des V. Le texte à coder est d'abord découpé en groupes de deux lettres à partir de la première. Si le nombre de lettres du texte est impair alors on ne code pas la dernière lettre. Ensuite, on code chaque couple de lettres en utilisant le principe décrit ci-dessous avec la grille donnée en exemple.

- a Si deux lettres sont sur la même ligne, on prend les deux lettres qui les suivent immédiatement à leur droite. Exemples : FJ sera remplacé par US et VE par EC.
- b Si deux lettres sont sur la même colonne, on prend les deux lettres qui les suivent immédiatement en dessous. Exemples : BJ sera remplacé par JL et RM par ID.
- c Si les deux lettres sont identiques, on les considère comme étant sur la même ligne, on prend donc, deux fois la lettre qui suit à droite. Exemples : AA sera remplacé par RR et ZZ par BB.
- d Si les deux lettres ne sont ni sur la même colonne ni sur la même ligne, elles sont donc sur les coins d'un rectangle, elles sont alors codées par les deux lettres figurant sur les deux autres coins du rectangle. La première des deux lettres codées est sur la même ligne que la première lettre à coder. Exemples : OK devient VA, BI devient DC, GO devient YV.

B	Y	D	G	Z
J	S	F	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

Mathilde et Maëlle utilisent ce système de codage avec la grille ci-dessus pour communiquer en toute discrétion.

- Aider Maëlle à coder le message suivant : JE PEUX JOUER DEMAIN MATIN
- Décoder le message que Mathilde lui a envoyé en réponse : PCYIOFSRMIITOPZIEIMIS
- Les filles ont dû changer leur grille de codage. Mathilde envoie JTFDXQSXEKKQIYRKLKLU qui veut dire PEUT ETRE SAMEDI SOIR.  
Compléter la grille ci-contre pour trouver la grille de codage utilisée par Mathilde.

		Z		
X				E
L	N			
O	C	M		
H	P	G	V	

### Exercice n°4 : (2010)

Ohobmsmo x°4

Kfymkd

5 zysxdc

Fyec ckfoj mobdksxowoxd aeo vo bkvvio wkdrówkdsaeo ne Moxdbo pôdo coc fsxqd-msxa kxc moddo kxxóo. Ox aeovvo kxxóo k oe vsoe vk zbowsòbo ozboefo yppsmsovvo no mo zbocdsqsoeh myxmyebc ?



### Exercice n°5 : (2012)



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Polybe, un historien grec (vers 200 – 125 av. J.-C.), est à l'origine du premier procédé de chiffrement par substitution. C'est un système de transmission basé sur un carré de 25 cases. Chaque lettre peut être ainsi représentée par un groupe de deux chiffres : celui de sa ligne suivi de celui de sa colonne.

Ainsi : "E" = 15, "U" = 51, "N" = 34 ...

Mais ce codage est peut-être un peu simple. On décale alors l'alphabet avec un mot de passe... Par exemple, si le mot de passe est ELECTRICITE, on commence à remplir le carré avec les lettres de ce mot, en ne gardant que la première occurrence de chaque lettre, ce qui donne E L C T R I, puis on complète le tableau avec les lettres inutilisées dans l'ordre alphabétique.

(voir ci-contre)

Le W n'est pas utilisé. Au besoin, on emploie le V à sa place.

	1	2	3	4	5
1	E	L	C	T	R
2	I	A	B	D	F
3	G	H	J	K	M
4	N	O	P	Q	S
5	U	V	X	Y	Z

Que se cache-t-il derrière le message chiffré ci-dessous ? Pour le découvrir, il faut le SESAME.

**41153212214531234244121431124422123413213413111112**

