
Jeux de cryptographie

Volume 1

Table des matières

Introduction	2
Énigmes	3
1 Pour bien commencer *	4
2 Message d'encouragement *	4
3 Alphabet mystérieux 1 *	5
4 Alphabet mystérieux 2 **	6
5 Gloire à l'empereur! *	7
6 Message d'un officier **	8
7 Nombres et géométrie ***	9
8 Opération anti-braconnage 1 *	10
9 Opération anti-braconnage 2 *	11
10 Opération anti-braconnage 3 **	11
Indices	12
Solutions	15

Introduction

Merci d'avoir téléchargé le premier volume du livre « Jeux de cryptographie » sur le site enigmatheque.com ! Ce livre numérique comporte 10 messages codés de niveaux de difficulté variés, symbolisés par des étoiles : facile (*), moyen (**), et difficile (***). Si vous rencontrez des difficultés pour déchiffrer un message, pas de panique, vous trouverez des indices aux pages indiquées en bas des énigmes. Si toutefois vous restez bloqué malgré les indices, vous pouvez consulter les solutions détaillées étape par étape à la fin du livre. Aussi, n'hésitez pas à faire des recherches sur internet et à utiliser des outils informatiques (tableur par exemple) si vous en ressentez le besoin.

Bon courage, et surtout amusez-vous bien !

Énigmes

#1 - Pour bien commencer *

Ce premier message codé a pour but de vous faire découvrir l'esprit du livre et la démarche à suivre pour les prochaines énigmes, qui seront bien sûr plus difficiles ! ;)

```
4 17 21 8 11   4 2   4 3   4 6 0 18 18 4 12   17 4 8 12 4 17
15   4 11   17 4 17 5 5 8 7 2 4 3   4 3   25 4 13 4 21   18 20
      14 21   18 13 14 8 19 0 19 8 2 8 11 4 5
```

Indice p.13 / Solution p.16

#2 - Message d'encouragement *

Cette fois-ci, le message n'est plus codé par des chiffres mais par des lettres. Parviendrez-vous à le déchiffrer ?

```
TC JF IM LH AA NI BD WD GF AA DJ DB BC SC EJ BB QB TF GJ RC KE
ID IG EC EQ BD BA HH IF KD BD AC GB AA LC BB CC FK JF RD MF DI
      AA IK BT FD EP BD
```

Indice p.13 / Solution p.16

#3 - Alphabet mystérieux 1 *

Les noms de sept mathématiciens célèbres ont été écrits dans un mystérieux alphabet. À vous de les décrypter et de les associer aux noms de la colonne de droite.

▽ ∩ ∠ ⊙ ∧ □ •	• Hilbert
○ ⊙ △ ⊠ ⊕ ∠ ▽ •	• Turing
□ ▽ ∩ ∩ ∩ •	• Galois
∠ ⊙ ⊕ ∩ ▽ ∩ ∩ •	• Neumann
□ ▽ △ ∩ ⊙ ∩ •	• Gauss
△ ⊕ ∠ ∩ ▽ ▽ •	• Riemann
∩ ⊕ ∩ ∩ ▽ ∩ ∩ •	• Fermat

#4 - Alphabet mystérieux 2 **

Pour cette énigme, on reprend le même principe que précédemment, mais en augmentant la difficulté. Cette fois-ci, il vous faut retrouver sept grandes villes du monde. Les symboles découverts à l'énigme précédente ne correspondent plus nécessairement aux mêmes lettres.

▽∧∧εψ□□ •	• Paris
▽∧Δ∇∧ •	• Vilnius
▽⊗∧⊕□ •	• Londres
∩∩ψ⊕□ •	• Tokyo
○⊕▽∧⊕⊗□ •	• Pékin
∠⊗⊕▽∧ •	• Tunis
∩□Δ⊕∧ •	• Quito

#5 - Gloire à l'empereur ! *

Les lettres ci-dessous codent une citation d'un célèbre empereur, tirée de son ouvrage « La guerre des Gaules » (Livre III). À vous de décoder cette citation !

EXL AHFFXL VKHBXGM OHEHGMBXKL VX JN BEL WXLBKXGM

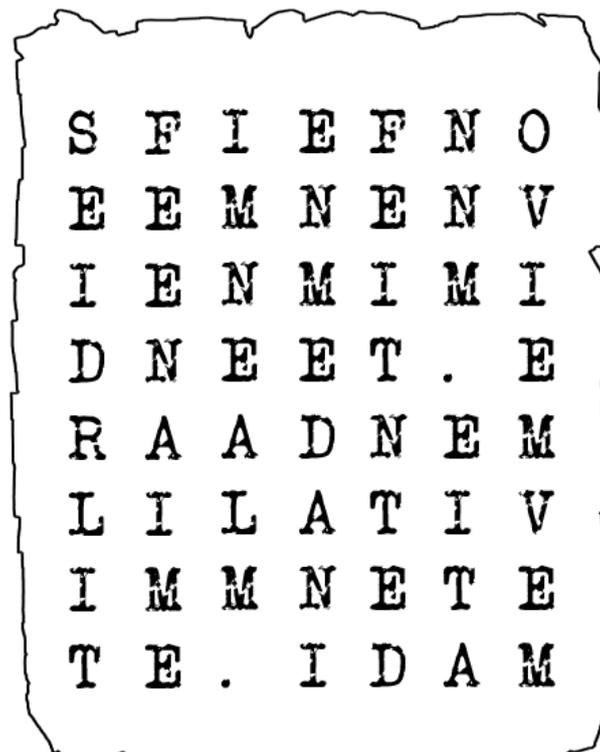
Le saviez-vous ?

L'empereur en question utilisait lui-même cette méthode de chiffrement avec une clé de 3 pour ses communications militaires avec Cicéron (ce qui explique le nom de la méthode).

Indice p.13 / Solution p.19

#6 - Message d'un officier **

Vous êtes un haut responsable de la logistique et de l'armement de l'armée française durant la première guerre mondiale. Un officier d'artillerie engagé en Picardie vous fait parvenir ce message en cette année de 1918.

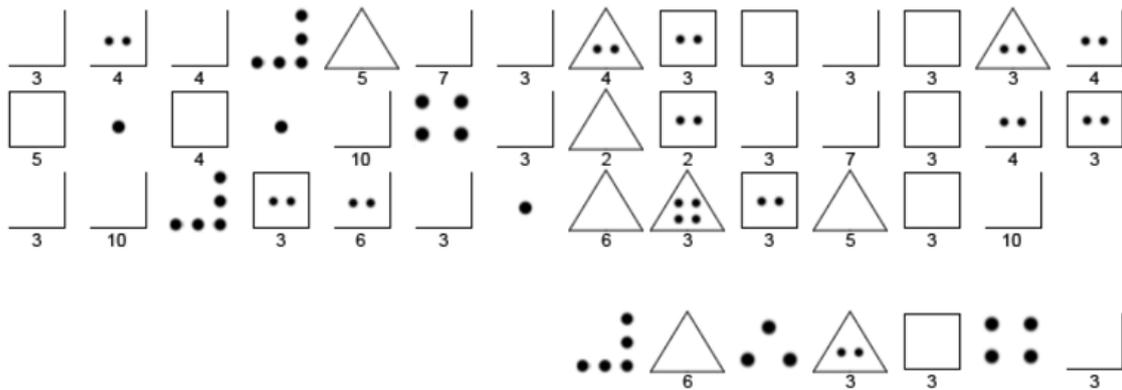


S	F	I	E	F	N	O
E	E	M	N	E	N	V
I	E	N	M	I	M	I
D	N	E	E	T	.	E
R	A	A	D	N	E	M
L	I	L	A	T	I	V
I	M	M	N	E	T	E
T	E	.	I	D	A	M

Ce message semble urgent, vous vous empressez de le déchiffrer...

#7 - Nombres et géométrie ***

Une citation d'un célèbre mathématicien de la Grèce antique se cache derrière ces mystérieux symboles liant nombres et géométrie. Le mathématicien en question est particulièrement connu pour son ouvrage « Éléments », qui énonce des principes fondamentaux de la géométrie et de l'arithmétique. À vous de jouer !



Indices p.14 / Solution p.21

#8 - Opération anti-braconnage 1 *

Mise en situation :

La série « Opération anti-braconnage » est une série de trois messages codés échangés au sein d'un vaste réseau de braconnage. Les douaniers français enquêtent depuis longtemps sur ce réseau et mènent actuellement une grosse opération de démantèlement. Ils savent qu'un des braconniers s'apprête à rentrer sur le territoire français après un voyage de deux semaines au Kenya. Ils le soupçonnent de transporter des dizaines de défenses d'éléphant dans le but de les revendre à un riche client parisien.

Les douaniers ont intercepté ce message codé envoyé par le braconnier en question aux autres membres du réseau. Ils font appel à vos compétences en cryptographie pour les aider à déchiffrer ce message.

Message :

JAVAIVAVINGTDAVEFAVENSAVESDAVELAVEPHAVANTAVETDAVIXC
AVORNAVESDAVERHAVINAVOCAVERAVOS.JAVEDAVECAVOLLAVED
AVENAVAIRAVOBAVIETJAVATTAVERRAVISCAVESAVOIRAVANAVEU
FHAVEURAVESAVATAVOULAVOUSAVEBLAVAGNAVAC.

Parviendrez-vous à décoder le message dans les temps ?

#9 - Opération anti-braconnage 2 *

Les douaniers n'ont malheureusement pas pu intervenir à temps pour arrêter le braconnier... Celui-ci est toujours en cavale et a envoyé un autre message à ses complices, que les douaniers ont réussi à intercepter. Encore une fois, ils vous font confiance pour les aider à déchiffrer ce message.

Message :

JAFEPAFASSAFELAFANAFUITSAFURTAFOULAFOUSAFE.JAFEPRAFEN
DSLAFETRAFAINDAFEMAFAINMAFATAFINPAFOURPAFARAFIS.VAFEN
AFEZMAFECHAFAFERCHAFERAFALAFAGAFARAFEMAFONTPAFARNAFA
SSAFEAQAFUATAFORZAFEHAFEURAFES.

Indice p.14 / Solution p.23

#10 - Opération anti-braconnage 3 **

Après avoir déchiffré le message précédent, vous avez immédiatement prévenu les douaniers qui se sont rendus sur place sans attendre. Le braconnier a envoyé un dernier message à ses complices qui étaient censés venir le chercher.

Message :

JREG MSEZ SKUD IBSN FAAI IMTP AERF RJEL TVEC RAPH ALRM LOEY
SQDZ OTUG AJNL IXEW RTSA IKLU SOOF NETI CBOR NSFELISM QUUS
EPLA ANMI APRX CGHY AANB DNIK SEEN NIEP VAOU UBSO RLEM
NKDS EAZQ PUAC SEAB LEAM GUAV RDES

Indice p.14 / Solution p.23

Indices

#1 - Pour bien commencer *

Indice :

Et si les nombres représentaient des lettres ?

#2 - Message d'encouragement *

Indice :

Il y a beaucoup de lettres, mais en somme, ce n'est qu'un peu de calcul mental.

#3 - Alphabet mystérieux 1 *

Indice :

Une analyse de la position et de la répétition des lettres devrait vous aider !;)

#4 - Alphabet mystérieux 2 **

Indice :

Comme pour l'énigme précédente, une analyse de la position et de la répétition des lettres vous aidera.

#5 - Gloire à l'empereur ! *

Indice :

Aliter

#6 - Message d'un officier **

Indice :

En temps de guerre, il faut parfois savoir remettre de l'ordre dans ses colonnes d'infanterie !

#7 - Nombres et géométrie ***

Indice 1 :

Il peut être utile de trouver le nom du mathématicien en question, en recherchant le titre de son ouvrage sur internet par exemple.

Indice 2 :

Des nombres figurés se cachent derrière certains symboles du message.

#8 - Opération anti-braconnage 1 *

Indice :

Le braconnier est au Kenya, mais il s'est déjà rendu sur l'île de Java et sait parler le javanais.

#9 - Opération anti-braconnage 2 *

Indice :

Le braconnier a mangé un piment rouge, il a la langue de feu !

#10 - Opération anti-braconnage 3 **

Indice :

Le braconnier aime vraiment les parasites !

Solutions

#1 - Pour bien commencer *

Les nombres du message codé représentent des lettres de l'alphabet, en choisissant par convention $A = 0, B = 1, \dots, Z = 25$. La correspondance entre les nombres et le rang des lettres de l'alphabet sera utilisée à de nombreuses reprises tout au long du livre. Le message codé est le suivant :

4 17 21 8 11 4 2 4 3 4 6 0 18 18 4 12 17 4 8 12 4 17 15 4 11
17 4 17 5 5 8 7 2 4 3 4 3 25 4 13 4 21 18 20 14 21 18 13 14 8 19 0
19 8 2 8 11 4 5

En associant chaque nombre à la lettre de l'alphabet correspondante, nous obtenons :

ervil ec ed egassem reimerp el rerffihced ed zenev suov snoitaticilef

Le message est écrit à l'envers. En le réécrivant dans le bon sens, nous lisons :

Félicitations vous venez de déchiffrer le premier message de ce livre

Réponse :

Félicitations, vous venez de déchiffrer le premier message de ce livre !

#2 - Message d'encouragement *

Le message codé est formé de plusieurs paires de lettres, dont la somme des rangs correspond aux lettres du message clair, en prenant par convention $A = 0, B = 1, \dots, Z = 25$. Déchiffrons les quatre premières paires à titre d'exemple :

TC (T = 19; C = 2) $\rightarrow 19 + 2 = 21 \rightarrow V$ JF (J = 9; F = 5) $\rightarrow 9 + 5 = 14 \rightarrow O$
IM (T = 8; C = 12) $\rightarrow 8 + 12 = 20 \rightarrow U$ LH (T = 11; C = 7) $\rightarrow 11 + 7 = 18 \rightarrow S$

Le premier mot du message est donc « Vous ». Il reste à faire de même pour toutes les autres paires de lettres.

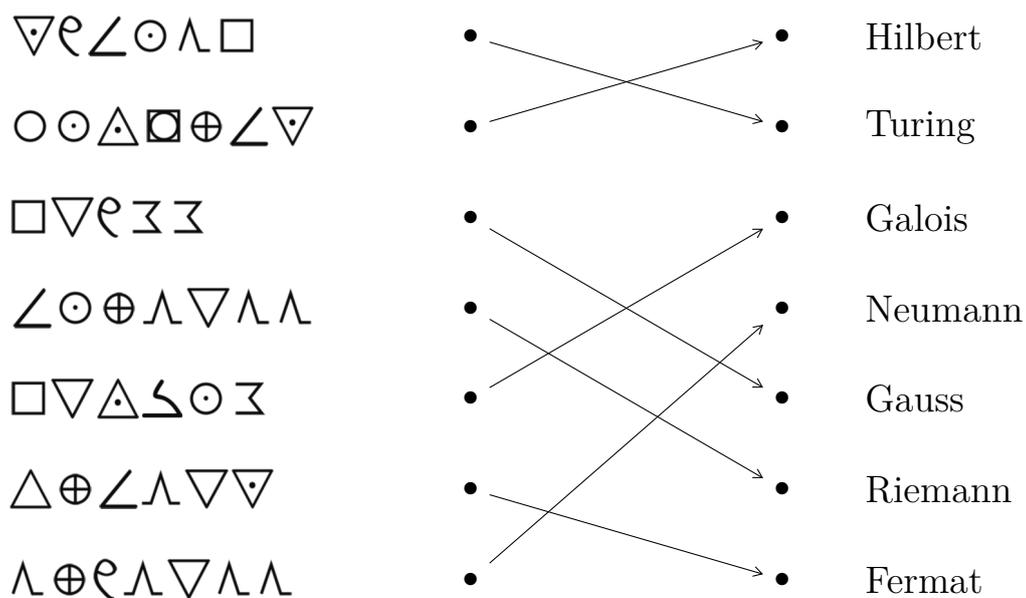
Réponse :

Vous avez l'âme d'un cryptologue. Bonne chance pour la suite !

#3 - Alphabet mystérieux 1 *

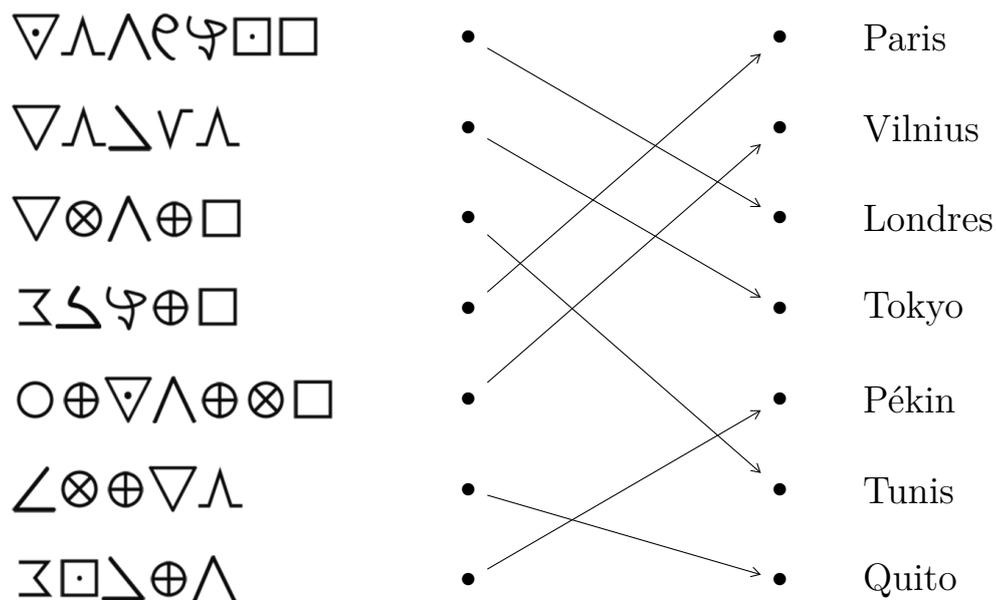
- Le dernier nom de la colonne de gauche est le plus facile à décrypter car il commence et se termine par la même lettre. Lorsque l'on regarde les noms de la colonne de droite, on voit qu'il n'y a que Neumann dont le nom commence et se termine par la même lettre. La dernière ligne cryptée est donc associée à Neumann.
- Les quatre dernières lettres de « Riemann » sont les mêmes que celles de « Neumann ». Par identification, on en déduit que Riemann est donc à la quatrième ligne de la colonne de gauche.
- Gauss est le seul nom de 5 lettres et est donc à la troisième ligne de la colonne de gauche.
- Le nom de Gauss décrypté précédemment a permis de trouver le symbole codant la lettre « G », qui est la dernière lettre de « Turing » et la première de « Galois ». Ces deux noms sont donc respectivement aux première et cinquième lignes.
- Il ne reste plus que Hilbert et Fermat à décrypter. La troisième lettre de « Fermat » est un « R », dont le symbole a été découvert lors de l'identification de Riemann. Par déduction, Hilbert est à la deuxième ligne et Fermat est à la sixième ligne.

Nous obtenons finalement les associations suivantes :



#4 - Alphabet mystérieux 2 **

Une démarche similaire à celle de l'énigme précédente permet d'obtenir les associations suivantes par identification des lettres et des symboles :



#5 - Gloire à l'empereur ! *

Le chiffrement utilisé pour cette énigme est le chiffrement César, qui est basé sur décalage des lettres de l'alphabet. Pour trouver le décalage, on peut tester les 25 clés possibles une par une, ou on peut essayer de trouver des mots ou des lettres probables. Une analyse fréquentielle permet de voir que le X est la lettre la plus courante dans le message, ce qui laisse penser qu'il code la lettre E, qui est la lettre la plus fréquente en français. Le décalage vaut donc 19. L'indice donnait ce décalage de manière implicite car « Aliter » se prononce comme « A lie T » et doit se comprendre par le fait que le A est codé par le T.

Un décalage de 19 donne l'alphabet de substitution suivant :

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

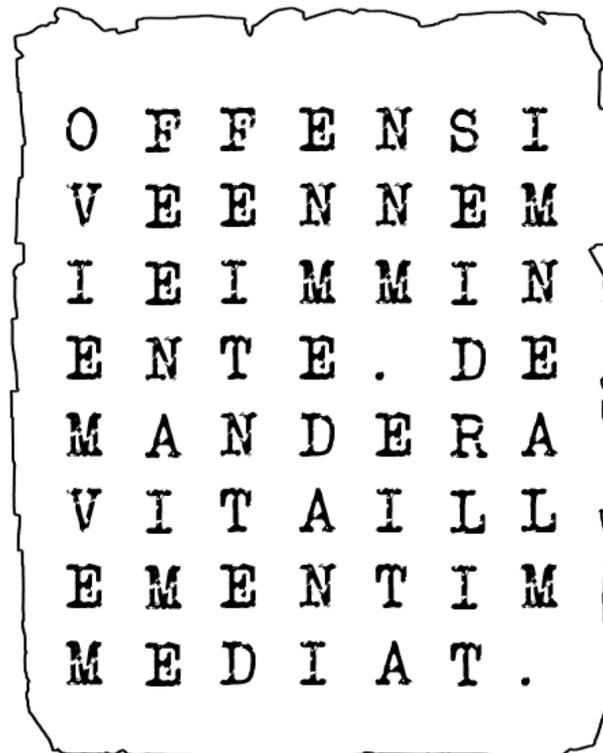
Il suffit de remplacer les lettres du message codé une par une pour déchiffrer la citation de Jules César.

Réponse :

LES HOMMES CROIENT VOLONTIERS CE QU'ILS DESIRENT

#6 - Message d'un officier **

Le message est presque écrit en clair, il suffit simplement de permuter correctement les colonnes pour le déchiffrer. Après avoir remis les colonnes dans le bon ordre, nous obtenons le message suivant :



O	F	F	E	N	S	I
V	E	E	N	N	E	M
I	E	I	M	M	I	N
E	N	T	E	.	D	E
M	A	N	D	E	R	A
V	I	T	A	I	L	L
E	M	E	N	T	I	M
M	E	D	I	A	T	.

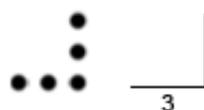
Réponse :

OFFENSIVE ENNEMIE IMMEDIATE. DEMANDE RAVITAILLEMENT IMMEDIATE

#7 - Nombres et géométrie ***

Les indices ne vous ont pas permis de déchiffrer la citation ? Voici une des démarches possibles pour la déchiffrer.

L'auteur de l'ouvrage « Éléments » est le célèbre mathématicien grec Euclide. Cet ouvrage est une ensemble de 13 livres comprenant des axiomes, des théorèmes, des définitions sur les fondements de la géométrie et de l'arithmétique. La mise en forme du message codé laisse penser que le dernier mot, en bas à droite, est l'auteur de la citation : « Euclide ». On remarque que la lettre « E » est codée par 2 symboles différents :



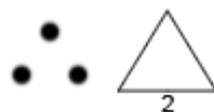
Le premier symbole est un angle droit formé de 5 points. Comme on sait qu'il code la lettre E (qui est la 5^e lettre de l'alphabet), on comprend que le nombre de points formant les symboles correspond à la position des lettres dans l'alphabet. Le symbole de droite est une représentation équivalente, sous forme condensée. Il s'agit là aussi d'un angle droit, et le nombre 3 signifie que les deux côtés sont constitués chacun de 3 points.

Il existe une formule générale donnant le nombre de points du symbole « angle droit » en fonction du nombre de point n d'un de ses côtés :

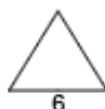
$$\text{Nombre de points} = 2n - 1$$

Le même principe de codage est utilisé pour les carrés et les triangles. Chacun des carrés et des triangles code un nombre, on parle respectivement de nombres carrés et triangulaires. D'autres nombres portent des noms de figures géométriques, comme les pentagones. De manière générale on parle de nombres figurés.

Les deux symboles suivants sont équivalents. Le premier symbole comporte trois points et représente un triangle ayant 2 points sur sa base. Il comporte au total 3 points et code donc la lettre C. Le symbole de droite en est une représentation condensée. Le chiffre 2 indique le nombre de points de la base.



De la même manière, le symbole représentant un triangle indicé du chiffre 6 :



est une forme condensée du triangle suivant, que l'on note T_6 .



Comme dans le cas de l'angle droit, il existe une formule reliant le nombre de points d'un triangle T_n au nombre de points n de sa base.

$$\text{Nombre de points} = \frac{n(n+1)}{2}$$

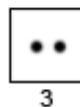
Le triangle T_6 comporte donc au total $\frac{6 \times 7}{2} = 21$ points et code donc la lettre U.

Le même raisonnement s'applique aux carrés. Le symbole représentant un carré indicé du chiffre 3 :



est une représentation compacte d'un carré dont les côtés sont formés de 3 points et comportant donc 9 points au total. Il code la lettre I. La formule générale reliant le nombre de points total au nombre de points n d'un côté est : n^2 .

Lorsqu'il y a des points à l'intérieur des symboles, cela signifie qu'il faut multiplier leur valeur par le nombre de points intérieurs. Ainsi, le symbole :



représente le chiffre $2 \times 9 = 18$ et code donc la lettre R.

Réponse :

En géométrie, il n'y a pas de chemin réservé aux rois. Euclide

#8 - Opération anti-braconnage 1 *

En analysant le message, on s'aperçoit que les lettres « AV » sont répétées de manière artificielle à de nombreuses reprises. Le braconnier a voulu brouiller le message en y ajoutant des lettres parasites afin de le rendre moins compréhensible. Si l'on supprime les « AV » parasites, nous obtenons directement le message clair. C'est le principe de codage du javanais, qui est un argot apparu en France au cours du XIXe siècle.

Réponse :

J'ai vingt défenses d'éléphant et dix cornes de rhinocéros. Je
décolle de Nairobi et j'atterris ce soir à neuf heures à Toulouse
Blagnac.

#9 - Opération anti-braconnage 2 *

Comme précédemment, le braconnier a brouillé son message en utilisant des lettres parasites. Cette fois-ci, c'est le groupement « AF » qui est parasite. Il suffit de retirer toutes ces lettres ajoutées artificiellement pour déchiffrer le message.

Réponse :

Je passe la nuit sur Toulouse. Je prends le train demain matin pour
Paris. Venez me chercher à la gare Montparnasse à quatorze heures.

#10 - Opération anti-braconnage 3 **

Une fois n'est pas coutume, le braconnier a brouillé son message en insérant des lettres parasites une fois sur deux. En enlevant les deuxième et dernière lettres de chaque groupe de quatre lettres, nous obtenons le message clair.

Réponse :

Je me suis fait arrêter par les douaniers. Ils ont confisqué la
marchandise. Ne vous rendez pas à la gare.