

Repérage par satellites:

Un homme est perdu dans le désert. Il dispose d'un système émetteur appelé G.P.S. (Global Positionnement System) . Ce système communique par émission d'ondes avec des satellites G.P.S.. Sachant qu'un satellite G.P.S. calcule la distance qui le sépare de l'émetteur, comment peut-on retrouver cet homme en utilisant le moins de satellites possible? Y-a-t-il une orbite privilégiée pour ces satellites?

Autour de π :

On désire estimer la constante π en calculant l'aire d'un disque. Peut-on retrouver π en utilisant uniquement des figures géométriques telles que le triangle équilatéral, le rectangle, le trapèze... dont on connaît l'aire exactement.

On se donne pour tout matériel une feuille de papier non quadrillée, une règle non graduée, un compas, un crayon de bois et une gomme (pour effacer les erreurs éventuelles). Peut-on construire un pentagone régulier? Un polygone régulier à 15 côtés?

Messages codés:

Voici trois messages codés différemment. À vous de retrouver les messages originels!

1. Premier message:

GNJS OTZJ, RFNSYJSFSY IJHWDUYJW HJ STZAJFZ RJXXFLJ : TI
BMKPVQYCM YCM DWCA DMVMH L'CBQTQAMZ A'IXXMTTM TM
KPQNNZM LM KMAIZ.

2. Deuxième message:

AJ UIO, H'ETVIBA BUPTOTVEOV E BUPTOFAMAM TAQEMANAPV HAT
BUPTUPPAT AV HAT WUYAHHAT.

3. Troisième message:

MLFH VHKVILMH JFV XV QVF ELFH Z ZNFHV. ELFH KLFEVA ZFHHR
XLMHGIFRIV VG XZHHVI WVH XLWZTVH KZI ELFH-NVNV.

Codage R.S.A.:

Le codage R.S.A. repose sur la factorisation d'un entier et donc sur les propriétés des nombres premiers.

Pour commencer, il faut convertir son texte en chiffres. Trouver une façon de convertir les 26 lettres de l'alphabet (en distinguant éventuellement les majuscules des minuscules), les lettres accentuées, la ponctuation, les espaces... à l'aide de chiffres.

Nous allons maintenant coder le message en codant chaque nombre représentant un symbole séparément.

Nous allons communiquer à toutes les personnes qui doivent nous envoyer des messages la « clé publique », il s'agit d'un couple (n, e) . Si n se décompose sous la forme $p \cdot q$ avec p et q premiers, on suppose en plus que e et $(p-1)(q-1)$ n'ont pas de facteur en commun. À partir d'un message que l'on note m , on obtient le message codé c en prenant le reste de la division euclidienne de m^e par n . Comment peut-on retrouver le message m ?

Essayer de crypter un message court avec la clé publique $(187, 7)$ et essayer de trouver la clé privée, c'est-à-dire de retourner au message initial.

Peut-on crypter des messages de toute taille?

Faire perdre à coup sûr:

Vous connaissez bien le jeu du « morpion ». On souhaite généraliser ce jeu: on se donne une grille de taille $d \times d$. Deux joueurs jouent chacun leur tour en cochant une case d'un rond ou d'une croix. Le gagnant est le premier qui aligne (horizontalement, verticalement ou en diagonal) n symboles (n est plus petit que d).

Peut-on établir une stratégie afin de faire perdre l'adversaire à coup sûr? Vous pouvez choisir la taille de la grille et regarder son influence sur le déroulement de la partie.

Comparer les stratégies entre le « morpion » et le jeu « puissance 4 ».