

1) Sociétal

a) Coder ou crypter

- Quelle est la différence entre les deux ?

Coder, c'est transformer une information pour permettre sa transmission d'une personne vers toutes les autres via une ou plusieurs machines. On utilise la plupart du temps des normes accessibles à tous.

Crypter, c'est transformer une information pour permettre sa transmission d'une personne vers un seul destinataire à l'exclusion de toute autre personne. On utilise des algorithmes et des « clés ».

<https://fr.wikipedia.org/wiki/Cryptographie>

https://fr.wikipedia.org/wiki/Codage_des_caractères

b) Situations

- M. A. et Mme B. se connaissent depuis longtemps et correspondent par courriel. M. A. habite en France et Mme B. dans un pays où l'usage d'Internet est fortement encadré. Ont-ils intérêt à utiliser des courriels chiffrés ?

Non, on voit immédiatement qu'un message est crypté.

La police du pays de Mme B. interviendra directement chez elle et lui demandera de s'expliquer.

Il faut mieux que le message transmis soit invisible (caché) dans un message anodin. On appelle ce procédé la stéganographie.

- M. C. et Mme D. collaborent pour préparer un sujet d'examen, mais n'habitent pas dans la même ville. Comment peuvent-ils faire pour échanger leurs projets de sujets en toute sécurité ?

Ils doivent utiliser une messagerie chiffrée. Par exemple *Thunderbird* avec *PGP* en utilisant chacun une paire de clés privée et publique. La clé publique sert à crypter un message qui ne peut être décrypté (lu) qu'avec la clé privée correspondante.

- M. E. fait beaucoup d'achats sur le réseau Internet. Il lui arrive même de commander à partir d'un ordinateur situé sur son lieu de travail. Prend-il des risques en utilisant sa carte bleue personnelle ?

Non en théorie s'il utilise des sites de paiement sécurisés. (https, , ...)

Oui en pratique, si le site initial ayant appelé le site de paiement n'est pas sécurisé, une attaque par détournement peut emmener M. E sur un site d'apparence similaire à un site sécurisé mais aux mains de pirates.

- M. G., mathématicien, est chercheur dans le domaine de la cryptographie. Il vient de mettre en place un nouvel algorithme de cryptage. Peut-il le publier sans compromettre la sécurité des futurs utilisateurs ?

Oui, il le faut absolument. La sécurité du cryptage doit reposer sur la ou les clés, exactement comme une serrure.

Connaître ses caractéristiques ne la rend pas moins sûre mais permet de connaître ses forces et ses faiblesses.

Il faut surtout prendre soin de la (des) clé(s).

2) Un exemple célèbre.

Tout le monde appelle la méthode ci-dessous, le « code César », alors que son but initial est de crypter :

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum uerbum effici posset: quae si qui inuestigare et persequi uelit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet. <i>Suétone, Vie de César LVI</i>	On a conservé en outre, ses lettres à Cicéron et celles qu'il adressait à ses familiers sur ses affaires domestiques. Quand il avait à leur faire quelque communication secrète, il usait d'un chiffre, c'est-à-dire qu'il brouillait les lettres de telle façon qu'on ne put reconstituer aucun mot. Si on veut en découvrir le sens et les déchiffrer, il faut substituer à chaque lettre la troisième qui la suit dans l'alphabet, c'est-à-dire le D à l'A et ainsi de suite.
---	--

a) Approche par le tableur,

On souhaite réaliser le cryptage de César avec un tableur : l'utilisateur saisit la phrase à coder et la clé de cryptage (correspondant au décalage) et la feuille calcule la phrase cryptée (le cryptogramme).

On travaillera dans toute l'activité avec des MAJUSCULES non accentuées !

- Ouvrez le fichier CryptageEleve.ods.
- Complétez les 3 cellules B9, E9 et H9 comme indiqué sur la feuille *Introduction*.
- Complétez les cellules B4 à B8 de la feuille *César* pour le décalage saisi en cellule B2.
- Vérifiez que le cryptage est correct.
- Recopiez ces cellules B4 à B8 vers la droite jusqu'à la colonne Y.
- Vérifiez que le cryptage de la colonne Y est correct.
- Quelle notion mathématique permet de « rester » dans les 26 lettres de l'alphabet ?
Le reste dans la division euclidienne est utilisé très fréquemment en cryptographie.

b) Sécurité ?

- Quel est le nombre de clés possibles ?
Il y a 25 clés car un décalage de 0 laisse le message en clair.
- Quelle lettre est la plus probable en français ?
La lettre « e » est la plus fréquente de la langue française.
- En quoi cela constitue-t-il une faille de sécurité pour ce type de codage ?
*Comme le « e » est toujours codé par la même lettre, trouver cette lettre donne la clé.
Il suffit de calculer les fréquences des lettres du message chiffré pour le savoir.*

c) Décrypter César

- Proposer une clé de **cryptage** qui appliquée à un message chiffré avec la clé 10 permet de le **décrypter**.
- Sélectionnez la plage de cellules B5:B8 et copiez collez là à partir de la cellule B17.
- Testez le décodage.
- Cette clé de décodage est-elle unique ?
Non, on peut utiliser -10, 16, -36, 42 ... tout entier de la forme $16 + 26k$ où $k \in \mathbb{Z}$.
- Vérifiez pour une valeur de la clé de codage différente de 10.

- Sauvegardez le fichier.

3) Un programme Python

Pour des textes plus longs, on se propose d'automatiser la procédure de cryptage de César en écrivant un programme en *Python*.

a) Aide pour Python.

- Convertir un entier (unicode) en un caractère est réalisé par la fonction `chr` :
Exemple : `chr(69)` renvoie la caractère E.
- Convertir un caractère en entier (unicode) est réalisé par la fonction `ord` :
Exemple : `ord('C')` renvoie l'entier 67.
- Convertir une chaîne de caractères en entier lorsque la chaîne représente un nombre est réalisé par la fonction `int` :
Exemple : `int('123')` renvoie l'entier 123. Le cas échéant, on peut préciser la base.
`int('2F', 16)` renvoie l'entier $45 = 2 \times 16 + 15$.
- Concaténer deux chaînes de caractères (ou une chaîne et un caractère).
On utilise l'opérateur `+`
Exemple : `Chaîne = "Jules " + "Cesar"` affecte "Jules Cesar" à la variable « Chaîne ».
- La boucle pour :

```
for i in range(n) :
```


 { Bloc d'instructions }
répète n fois le Bloc d'instructions.
L'entier « i » comptant les boucles, varie de 0 **inclus** à n **exclus** par pas de 1.
- La boucle pour bis :

```
for car in chaîne :
```


 { Bloc d'instructions }
répète le Bloc d'instructions pour chaque caractère dans la chaîne, en allant de gauche à droite.
- Obtenir le reste de la division Euclidienne.
On utilise l'opérateur `%`.
`a = 55 % 26` affecte 3 à la variable « a ». 55 divisé par 26 donne 2 avec comme reste 3.

4) Questionnaire de fin

Qu'as tu fait pendant cette heure ? (2 lignes maximum)

Qu'as tu appris pendant cette heure ?

Qu'est-ce que le principe de Kerckhoffs ?

Le principe de Kerckhoffs est que le système de chiffrement est public, que sa sécurité ne repose pas sur le secret de celui-ci mais sur le secret de la clé.

Que vaut $135[26]$? et $7 \times 65 + 78 [128]$?

$135[26]=5$ car $135=5 \times 26 + 5$

$7 \times 65 + 78[128] = 554[128] = 42$ car $554 = 4 \times 128 + 42$

Quel pourrait être l'intérêt d'un cryptage modulo 128 ?

Toutes les opérations sur les codes des caractères (Majuscules, minuscules, retour chariot, nombres, ...) dans la table ascii pourrait être « ramenées » dans la table ascii. On pourrait ainsi crypter des documents complets et pas seulement le texte. Il faut bien sûr que la suite d'opérations (le cryptage) puisse être inversée (décoder) La liste des opérations pour décoder est la clé de décodage.

5) Défis

a) En groupe

- Si besoin, communiquez par e-lyco pour vous répartir des tâches.
- Tentez de décrypter le message ci-dessous :

YNEVGUZRGVDHRQRYUBEYBTRFRERSRERNYNQQVGVBAQRFURHERFVAQVDHRRFCNEYNCRGV
GRNVTHVYYRQHARUBEYBTRPBAPERGRZRAGFVABHFPBZZRAPBAFNARHSURHERFRGNWBHGB
AFDHNGERURHERFNYBEFCYHGBGDHRQRGREZVARENGERVMRURHERFPBZZRQNAFYNNQQVGV
AABEZNYRABHFFBZZRFNHARURHERPBZZRRPEVERARHSCYHFDHNGERSBAGHAANCNFQRFRAF
BAQVGARHSCYHFDHNGERRFGPBATEHNHAZBQBHYBQBHMR

Une analyse fréquentielle nous indique qu'il s'agit d'une permutation des lettres.

La fréquence du « e » montre que la clé est 13.

ou bien on utilise la force brute qui consiste à utiliser toutes les clés possibles.

```
c = "YNEVGUZ ... MR"
for i in range(26):
    print (i)
    code(c, i)
    print()
```

LARITHMETIQUEDELHORLOGESEREFEREALADDITIONDESHEURESINDIQUEESPARLAPETITEAIGU
ILLEDUNEHORLOGECONCRETEMENTSINOUSCOMMENCONSANEUFHEURESETAJOUTONSQUATR
EHEURESALORSPLUTOTQUEDETERMINERATREIZEHEURESCOMMEDANSLADDITIONNORMALEN
OUSSOMMESAUNEHEURECOMMEECRIRENEUFPLUS

soit en rétablissant l'accentuation et la ponctuation :

L'arithmétique de l'horloge se réfère à l'addition des heures indiquées par la petite aiguille d'une horloge. Concrètement si nous commençons à neuf heures et ajoutons quatre heures alors plutôt que de terminer à treize heures comme dans l'addition normale nous sommes à une heure comme écrire neuf plus

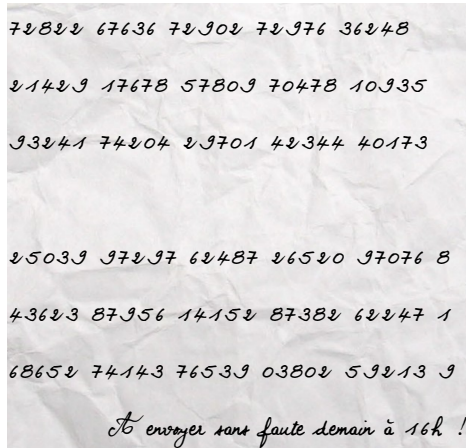
b) Une énigme à résoudre.

Les services de renseignements ont intercepté un message manifestement crypté donc voici le contenu :

Document 1 : 932417420429701423444017368652741437653903802592139

On a par ailleurs récupéré dans les affaires d'un espion deux documents dont voici des copies.

Document 2 :

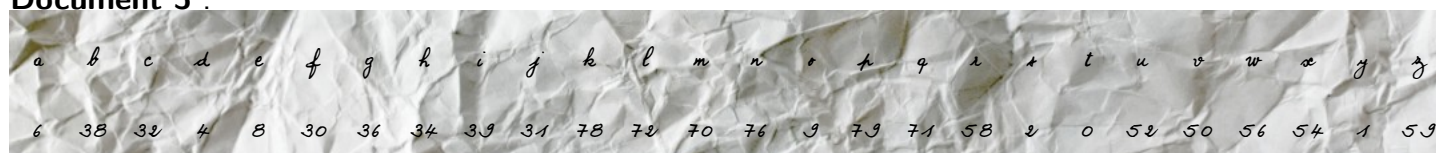


72822 67636 72902 72976 36248
21429 17678 57809 70478 10935
93241 74204 29701 42344 40173

25039 97297 62487 26520 97076 8
43623 87956 14152 87382 62247 1
68652 74143 76539 03802 59213 9

À envoyer sans faute demain à 16h !

Document 3 :



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
6	38	32	4	8	30	36	34	39	31	78	72	70	76	9	79	71	58	2	0	52	50	56	54	1	59

- Décodez le message.
Lessanglotslongsdesviolonsdelautomne
Les sanglots longs de violons de l'automne.
- Expliquez la méthode de cryptage.
Le texte est chiffré avec le document 3.
Un masque de la longueur du message est ajouté chiffre à chiffre modulo 10.
Le résultat est le document crypté
- Utilise-t-elle la notion mathématique évoquée au 2a) ?
Oui, l'addition est réalisée modulo 10. On n'utilise pas la retenue.
- Qu'appellera-t-on la clé ici ?
La clé est le masque ajouté au message :
21429 17678 57809 70478 10935 43623 87956 14152 87382 62247 1
Pour décrypter, on retire la clé modulo 10.
- Quelle précaution doit-on prendre pour la sécurité de cette méthode ?
Il faut que la clé reste secrète.
- Cherchez des explications simples sur le *code du Che* et le *masque de Vernam*.
Le Code utilisé par Che Guevara et Fidel Castro pour communiquer est une variante du masque de Vernam.
La première transposition en nombre n'apporte pas de sécurité supplémentaire. Ils auraient pu coder A par 1, B par 2, etc. et travailler modulo 26 sans perdre en sécurité.

Par contre, le masque doit être aléatoire et utilisé une seule fois pour que la sécurité soit totale.

- Vidéo

Le système RSA est asymétrique.

La connaissance de la clé de cryptage ne permet pas de trouver la clé de décryptage.

Ainsi on peut rendre la clé de cryptage public. Toute personne peut envoyer un message crypté au possesseur de la clé de décryptage qu'il doit garder privée.