scienceinfuse

ANTENNE DE FORMATION ET DE PROMOTION DU SECTEUR SCIENCES & TECHNOLOGIES

DOSSIER ENSEIGNANT

π

MATHS

Une introduction à la cryptographie

UCL **Scienceinfuse** - Antenne de formation et de promotion du secteur sciences & technologies
rue des Wallons 72 L6.02.01 - 1348 Louvain-la-Neuve

La **cryptographie** est utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Elle désigne l'ensemble des techniques permettant de chiffrer (ou coder) des messages, c'est-à-dire permettant de les rendre incompréhensibles.

La **cryptanalyse** est la reconstruction d'un message chiffré en clair (ou décodage) à l'aide de méthodes mathématiques.

La **cryptologie** est la science qui étudie les aspects scientifiques de ces techniques, c'est-à-dire qu'elle englobe la cryptographie et la cryptanalyse. La cryptologie est essentiellement basée sur l'arithmétique.

Exemple :

"OPVTBUUBRVPOTEFNBJO"

signifie

"Nous attaquons demain"

Pour comprendre ce message il faut connaître la clé qui a servi à le coder.

Nous allons voir ici deux types de chiffrement. Il en existe beaucoup d'autres.

1 Chiffrement par décalage

Jules César ne faisait pas confiance à ses messagers lorsqu'il envoyait des messages à ses généraux. Il chiffrait ses messages en remplaçant tous les "A" par des "D", les "B" par des "E" et ainsi de suite. Seule la personne connaissant la clé correspondant au nombre de caractères de décalage (ici 3) pouvait déchiffrer ses messages.

Activité 1 : En utilisant les bandelettes et le code secret de Jules César, chiffrez le mot "bonjour" et déchiffrez la phrase "frpphqw ydv-wx ?"

Placer les élèves par deux et donner à chaque groupe une grande et une petite bandelette. Il faut mettre la grande bandelette à gauche et la petite à droite et aligner le "A" du milieu de la grande bandelette avec le "D" de la petite bandelette. Le codage se fait de gauche à droite et le décodage de droite à gauche.

Si on décale de 3 l'alphabet	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
on obtient	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
et donc	B O N J O U R
devient	E R Q M R X U
et	F R P P H Q W Y D V – W X ?
signifie	C O M M E N T V A S – T U ?

L'avantage de ce procédé est qu'il est facile à utiliser pour coder les messages.
Son inconvénient est que les messages codés par ce procédé sont faciles à décoder. En effet,

- les mêmes lettres sont codées par des mêmes lettres (par exemple les deux "O" dans "bonjour") ;
- même si on ne connaît pas la clé, il n'y a que 25 possibilités de décaler les lettres de l'alphabet.

Un autre procédé de chiffrement consiste à retourner l'alphabet puis décaler les lettres.

Activité 2 : A l'aide des bandelettes, utilisez ce procédé avec un décalage de 5 pour chiffrer le mot "bonjour".

Placer les élèves par deux et donner à chaque groupe une grande et une petite bandelette.
Il faut mettre la grande bandelette à gauche et la petite à droite et retourner la petite bandelette. Aligner le "A" du milieu de la grande bandelette avec le "U" de la petite bandelette.
Le codage se fait de gauche à droite.

Si on renverse l'aphabet	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
on obtient	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
puis on décale de 5	U T S R Q P O N M L K J I H G F E D C B A Z Y X W V
et donc	B O N J O U R
devient	T G H L G A D

Ce procédé est facile à utiliser pour coder les messages. De plus, les messages codés par ce procédé sont plus difficiles à décoder que par le code de Jules César si on ne pense pas à retourner d'abord l'alphabet.
Cependant, les messages codés par ce procédé sont quand même faciles à décoder. En effet,

- les mêmes lettres sont codées par des mêmes lettres (par exemple les deux "O" dans "bonjour") ;
- si on sait qu'il faut d'abord retourner l'alphabet, il n'y a que 26 possibilités à essayer.

2 Chiffrement cyclique

Pour que les messages soient plus difficiles à décoder on peut utiliser le **chiffrement cyclique**.
Il s'agit de décaler les lettres de l'alphabet mais en changeant le décalage à chaque lettre.
Pour cela, il faut choisir un **mot-clé** qui nous indiquera le décalage à effectuer.
Par exemple, le mot-clé "SCIENCES" signifie que pour décoder la première lettre on aligne "A" avec "S", pour décoder la deuxième lettre on aligne "A" avec "C", pour décoder la troisième lettre on aligne "A" avec "I" et ainsi de suite. Après la huitième lettre (fin du mot SCIENCES), on recommence "A" avec "S",...

Activité 3 : A l'aide du mot-clé "SCIENCES", chiffrez le mot "bonjour".

Cette activité peut se faire à l'aide des bandelettes mais est plus facile avec un disque de chiffrement.

Avec les bandelettes : il faut mettre la grande bandelette à gauche et la petite à droite et aligner le "A" du milieu de la grande bandelette avec le "S" de la petite bandelette pour la première lettre, puis aligner le "A" du milieu de la grande bandelette avec le "C" de la petite bandelette pour la deuxième lettre et ainsi de suite. Le codage se fait de gauche à droite.

Avec le disque de chiffrement : les lettres à coder se trouvent sur le disque de couleur. A chaque lettre, aligner le "A" du disque de couleur avec la lettre correspondante du mot-clé sur le disque blanc. Le mot codé est construit en utilisant les lettres du disque blanc.

On place le "S" en face du "A" et donc "B" devient "T".
On place le "C" en face du "A" et donc le "O" devient "Q".
On place le "I" en face du "A" et donc le "N" devient "V".
On place le "E" en face du "A" et donc le "J" devient "N".
On place le "N" en face du "A" et donc le "O" devient "B".
On place le "C" en face du "A" et donc le "U" devient "W".
On place le "E" en face du "A" et donc le "R" devient "V".

Le mot "BONJOUR" est donc codé par "TQVNBWV".

Les avantages de ce procédé sont les suivants :

- il est facile à utiliser pour coder les messages ;
- les mêmes lettres sont codées par des lettres différentes (par exemple les deux "O" dans "bonjour") ;
- des lettres différentes sont codées par les mêmes lettres (par exemple "N" et "R" sont toutes les deux codées par "V" dans "bonjour").

Les messages codés par ce procédé sont très difficiles à décoder si on ne connaît pas le mot-clé.

Activité 4 : A l'aide du mot-clé "TRESOR", décodez les messages sur les parchemins. Ceux-ci vont vous permettre de trouver le numéro du cadenas qui ouvre le coffre aux trésors...

Pour cette activité, utiliser les bandelettes ou le disque de chiffrement.
Il y a 2 parchemins (numérotés 1 et 2). Placer les élèves par groupes de 4 et donner un parchemin pour 2 élèves, de sorte que chaque groupe de 4 élèves puisse trouver le code du cadenas. Quand tous les groupes ont trouvé le code, ouvrir le coffre.

!!! Ne pas oublier de mettre un trésor (bonbons,...) dans le coffre avant l'activité !!!
Le code du cadenas est 4130.