scienceinfuse

ANTENNE DE FORMATION ET DE PROMOTION DU SECTEUR SCIENCES & TECHNOLOGIES

DOSSIER ELEVE

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 ?"

Le mot B O N J O U R
devient

et F R P P H Q W Y D V – W X ?
signifie

Avantages de ce procédé :

Inconvénients de ce procédé :

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".

Le mot	B O N J O U R
devient	

Avantages de ce procédé :

Inconvénients de ce procédé :

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".

Le mot	B O N J O U R
devient	

Avantages de ce procédé :

Inconvénients de ce procédé :

Conclusion :

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...

Texte sur le Parchemin 1 :

Texte sur le Parchemin 2 :

Numéro du cadenas :