Les clés du numérique

défi CRYPTOGRAPHIE

FICHE ENSEIGNANT

Envoyer un message secret

INTRODUCTION

Comment coder et décoder un message secret ? La cryptographie est l'ensemble des techniques qui permettent de chiffrer et de déchiffrer un message, dont le contenu ne doit être connu que de son expéditeur et de son destinataire. C'est une science d'actualité, surtout avec Internet et toutes les précautions qui doivent être prises pour garantir la sécurité des communications. Au cours des siècles de nombreux systèmes cryptographiques ont été mis au point, de plus en plus perfectionnés, de plus en plus astucieux ! Les méthodes de codage sont nombreuses. Nous proposons aux élèves d'expérimenter deux exemples.

COMPÉTENCES / LIENS AVEC LES PROGRAMMES

Mathématiques

- Calculer avec les nombres entiers (utilisation de tableaux à double entrée à compléter, pour lire des informations et organiser des données)
- Résoudre des problèmes mettant en jeu les opérations arithmétiques

Outils numériques pour échanger et communiquer

L'élève sait mobiliser différents outils numériques pour créer des documents intégrant divers médias et les publier ou les transmettre, afin qu'ils soient consultables et utilisables par d'autres.

MATÉRIEL

- Une fiche élève « Envoyer un message secret » (page 6)

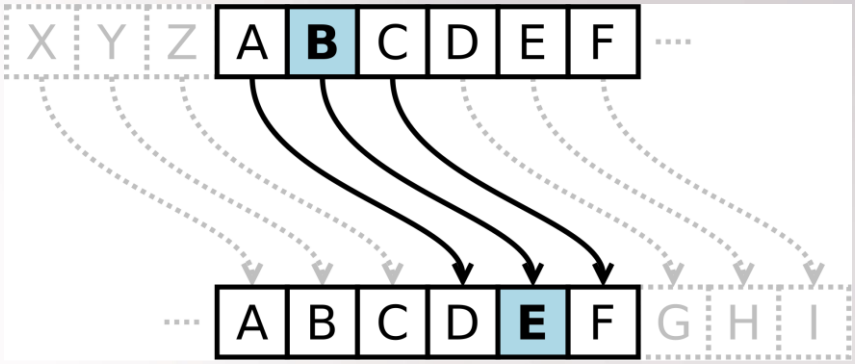
DÉROULEMENT DE L'ACTIVITÉ

Introduire l'activité en disant que l'on va découvrir la cryptographie, cette science qui étudie des façons de coder et décoder des messages secrets…

1 / Le chiffre de César

Le chiffre de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Voici le principe de la méthode : le texte codé s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située x rangs plus loin dans l'alphabet. La longueur du décalage constitue la clé du chiffrement. Le code de César a la particularité qu'il est basé sur un simple décalage de l'alphabet.

Jules César utilisait cette technique pour certaines de ses correspondances, notamment militaires, comme avec Ciceron. Exemple avec une clé de cryptage égale à 3 :



Avec une clé de cryptage égale à 3 (figure ci-dessus), le mot NUMERIQUE est codé par QXPHULTXH. Avec la même clé de cryptage, proposer aux élèves de crypter leur prénom et de répondre aux questions de la fiche élève.

- Décrypter le mot ERQMRXU => **BONJOUR**

- Décrypter le texte suivant sachant que la clé de codage est 10 : EBQOXD OVSWSXOB VK MSLVO => **URGENT ELIMINER LA CIBLE**

- Décrypter le texte suivant en supposant que le mot "ennemi" y figure : STYWJ JSSJRN IJ YTZOTZWX JXY IJ WJYTZW => **NOTRE ENNEMI DE TOUJOURS EST DE RETOUR (Clé 5)**

- Le mot AJMQAPA a été crypté mais on ignore la clé de cryptage => **ENQUETE (clé 22)**

- La grande faiblesse du chiffre de César réside dans le fait qu'il y a trop peu de clefs possibles : comme il y a 26 lettres dans l'alphabet, il n'y a que 25 décalages intéressants (un décalage de 26 redonne le message initial). Il suffit donc d'essayer tous les décalages pour trouver le bon !

2 / Un message à clé

Très rapidement, on se rend compte que les experts peuvent facilement décoder les messages où chaque lettre est toujours représentée par un même symbole. On a donc inventé d'autres formes de codification ou de cryptage.

L'utilisation d'une clé est l'une des formes qui ont été développées au cours des années. Une clé est habituellement une série de chiffres d'une longueur donnée. La clé est réutilisée autant de fois qu'il est nécessaire pour coder toutes les lettres du message. Cette clé doit être connue uniquement du rédacteur du message et de la personne qui le reçoit. Elle est utilisée pour qu'une certaine lettre ne soit pas toujours remplacée par la même lettre dans le message. Ainsi, la lettre A peut être remplacée par C une fois, puis par D plus loin dans le message.

Voyons comment cela fonctionne en utilisant la clé: 35412. Le message à coder est : *CODE SECRET*. On place d'abord les lettres à coder par groupe de 5, CODES ECRET

Le message à coder	C	O	D	E	S		E	C	R	E	T
Rang dans l'alphabet	3	15	4	5	19		5	3	18	5	20
Clé	3	5	4	1	2		3	5	4	1	2
Somme des 2 nombres	6	20	8	6	21		8	8	22	6	22
Retour aux lettres	F	T	H	F	U		H	H	V	F	V

Étape 1 : Placer les lettres du message à coder en groupe de 5 (car la clé est à 5 chiffres).
Étape 2: Identifier le rang dans l'alphabet associé à la lettre à coder.
Étape 3: Inscrire dans les cases les chiffres de la clé. Un seul chiffre doit être écrit dans chaque case.
Étape 4: Faire la somme du nombre de l'étape 2 et de la clé.
Étape 5: Trouver la lettre associée au nombre trouvé, qui correspond à sa place dans l'alphabet

Quand la somme donne un nombre plus grand que 26, on enlève 26 pour trouver le rang de la lettre que l'on va utiliser. (30 – 26 = 4)

On remarque que les mêmes lettres du message à coder ne se traduisent pas par la même lettre dans le message codé.

Le message codé est donc : FTHFU HHVFV

Pour décoder, un message, on procèdera de la même façon mais il faudra soustraire les nombres au lieu de les additionner. Voyons notre message codé que l'on veut maintenant décoder. La clé est 35412.

Le message codé	F	T	H	F	U		H	H	V	F	V
Rang dans l'alphabet	6	20	8	6	21		8	8	22	6	22
Clé	3	5	4	1	2		3	5	4	1	2
Différence des 2 nombres	3	15	4	5	19		5	3	18	5	20
Retour aux lettres	C	O	D	E	S		E	C	R	E	T

Le message décodé est : Code secret

Si le nombre associé à la lettre codé est égal ou plus petit que celui de la clé, on lui additionnera 26 avant de faire la différence.

Proposer maintenant aux élèves de décoder le message codé : TIOFH BZPWV IESGG GPZQQ. La clé est 24123. Le message original est **RENDEZ VOUS GARE DE LYON**.

Toutefois le codage à clé pose un autre problème car il s'agit d'un codage symétrique : si vous savez coder les messages, alors vous savez aussi automatiquement les décoder. Donc si un espion parvient à se procurer la clé que vous donnerez à votre ambassadeur, alors l'ennemi saura ensuite décrypter les messages qu'il vous enverra !

La solution pour s'en sortir est d'utiliser une méthode de cryptographie asymétrique, c'est-à-dire où les procédures de codage et de décodage sont très différentes, de sorte que quelqu'un qui sache encoder les messages ne sache pas pour autant les décoder. Comment est-ce possible ?

Un algorithme* asymétrique fait appel à deux clés : une clé dite « publique » qui sert à encoder le message, et une clé dite « privée » qui sert à le décoder. Donc si vous êtes le chef de la diplomatie, vous expédiez une clé publique à votre ambassadeur, et vous gardez pour vous la clé privée correspondante. Vos diplomates pourront encoder les messages, mais s'ils se font voler la clé publique, l'ennemi ne pourra pas pour autant décoder vos communications, car seule la clé privée permet de le faire !

**Un algorithme, c'est tout simplement une façon de décrire dans ses moindres détails comment procéder pour résoudre un problème ou obtenir un résultat donné (recette de cuisine, instructions très précises pour un robot totalement dénué de pensée…)*

3 / Envoyer un message crypté à fers@fers.asso.fr

Une fois que les élèves ont découvert différentes façons de crypter des messages, nous vous proposons d'écrire un message, de le crypter puis d'envoyer le message crypté à fers@fers.asso.fr

N'oubliez pas de préciser les indices à communiquer, indispensables pour décrypter le message ou de répondre aux demandes d'aide en renvoyant d'autres indices (clé utilisée par exemple)

Ensuite, il faudra vérifier si le ou les messages décryptés sont corrects et féliciter la personne ou la classe qui aura trouvé. Nous pourrons alors vous proposer de décrypter à votre tour les messages des autres classes.

Il est aussi tout à fait possible d'appliquer un codage binaire au message crypté, c'est-à-dire de le numériser. En effet, lors de l'activité transmission de données, les élèves ont réfléchi à la façon de coder l'alphabet avec 5 bits (1=A, 2=B, etc.) comme indiqué dans le tableau ci-dessous :

Code binaire	**00001**	**00010**	**00011**	**00100**	**00101**	**00110**	**00111**	**01000**	**01001**
Nombre	1	2	3	4	5	6	7	8	9
Alphabet	A	B	C	D	E	F	G	H	I

Code binaire	**01010**	**01011**	**01100**	**01101**	**01110**	**01111**	**10000**	**10001**	**10010**
Nombre	10	11	12	13	14	15	16	17	18
Alphabet	J	K	L	M	N	O	P	Q	R

Code binaire	**10011**	**10100**	**10101**	**10110**	**10111**	**11000**	**11001**	**11010**
Nombre	19	20	21	22	23	24	25	26
Alphabet	S	T	U	V	W	X	Y	Z

Pour cela, il est souhaité que les élèves aient écrit en binaire tous les nombres de 0 à 31 avec un codage binaire de l'alphabet sur 5 bits, par exemple A = 00001 ; B = 00010, etc.

Sources :

www.smac.ulaval.ca/

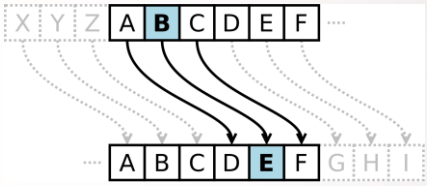
POUR ALLER PLUS LOIN

À l'attaque des codes secrets
Article de la revue de culture scientifique en ligne, Interstices, créée par des chercheurs pour vous inviter à explorer les sciences du numérique.
https://interstices.info/jcms/i_53837/a-l-attaque-des-codes-secrets

dCode
Site pour décoder ou encoder des messages avec les techniques de cryptographie classiques.
http://www.dcode.fr/

Envoyer des messages secrets

Le chiffre de César



Le texte codé s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située trois plus loin dans l'alphabet. La longueur du décalage constitue la clé du chiffrement.

- Avec une clé de cryptage égale à 3 (figure ci-dessus) crypter votre prénom et décrypter le mot ERQMRXU :

- Décrypter le texte suivant sachant que la clé de codage est 10 : EBQOXD OVSWSXOB VK MSLVO

- Décrypter le texte suivant en supposant que le mot "ennemi" y figure :
STYWJ JSSJRN IJ YTZOTZWX JXY IJ WJYTZW

- Le mot AJMQAPA a été crypté mais on ignore la clé de cryptage. Saurez-vous la trouver et décrypter ce mot ?

- Expliquer les faiblesses d'un tel système de chiffrement.

Un message à clé

Pour coder un message avec une clé (série de chiffres d'une longueur donnée), il faut suivre plusieurs étapes décrites dans la première colonne du tableau. La clé est 35412. Essaie de coder le message : CODE SECRET. On place d'abord les lettres à coder par groupe de 5…

1) Le message à coder	C	O	D	E	S		E	C	R	E	T
2) Rang dans l'alphabet											
3) Clé	3	5	4	1	2		3	5	4	1	2
4) Somme des 2 nombres											
5) Retour aux lettres											

Le message codé est donc :

Voyons maintenant un message déjà codé que l'on veut décoder.

Pour décoder, un message, on procèdera de la même façon mais il faudra soustraire les nombres au lieu de les additionner. Si le nombre associé à la lettre codé est égal ou plus petit que celui de la clé, on lui additionnera 26 avant de faire la différence.

La clé est 24123 et vous avez reçu le message suivant : TIOFH BZPWV IESGG GPZQQ

1) Le message codé	T	I	O	F	H		B	Z	P	W	V
2) Rang dans l'alphabet											
3) Clé											
4) Différence des 2 nombres											
5) Retour aux lettres											

1) Le message codé	I	E	S	G	G		G	P	Z	Q	Q
2) Rang dans l'alphabet											
3) Clé											
4) Différence des 2 nombres											
5) Retour aux lettres											

Ecrivez le message original :