VISIT MATH

Cofinancé par l'Union européenne

Le codage

Sujet	Algorythmes.
Objectifs d'apprentissage	Connaître les différentes façons de coder et apprendre à décoder.
Tranche d'âge	12 à 16 ans (à adapter à chaque pays).
Durée estimée	45 min.
Activités	Apprendre à coder et à décoder.
Visites associées	Paris, Beaumont-de-Lomagne, Centre de Varsovie, Athènes, Pise, Montauban.

Connaissances préalables requises

Aucun pré-requis particulier nécessaire

Étape par étape : la séquence en classe

Étape 1 : Introduire le sujet

Brève présentation des éléments contextuels de cette séquence

La cryptographie est une science, entre les mathématiques et l'informatique, mais aux applications très concrètes. Elle a pour but de protéger des informations ; pour cela, le plus souvent, elle les rend apparemment incompréhensibles en les mélangeant et les transformant selon une certaine méthode.

Un peu d'Histoire :

- De -800 à -200 avant JC : Les Spartiates utilisaient des scytales
- Vers -600 avant JC : Nabuchodonosor utilisait des crânes rasés
- Vers -480 avant JC: Dematarus (Grec) isolé en Perse utilise des tablettes de cire pour prévenir son pays des projets de Xerxes (Perse)
- -100 / -44 avant JC : Chiffre de César (décalage alphabétique)

- 1er siècle : Apparition de l'encre invisible (fluides organiques riches en carbone)
- 1580 : Chiffre par substitution de symboles (Code nomenclature) - Marie Stuart
- 1586 : Traité des chiffres : Chiffre de Vigenère
- 1930 : Machine Enigma
- Fin 20e : Apparition du chiffrement à clé publique - RSA

Définition du codage

Cryptologie : Science regroupant la cryptographie et la cryptanalyse.

Cryptographie : Science visant à créer des cryptogrammes.

Cryptanalyse : Science analysant les cryptogrammes en vue de les déchiffrer.

Cryptogramme : Message chiffré.

Chiffrer / Coder / Crypter : Transformer un texte, une information en remplaçant les lettres (ou des mots pour coder) dans une écriture faites de signes prédéfinis.

Déchiffrer / Décoder : transformer un message chiffré en un message chiffré en un message clair conforme à l'original.

Décrypter : trouver le chiffre utilisé dans le cryptogramme.

Texte clair : Message original avant chiffrement.

Texte chiffré : texte obtenu après chiffrement.

Clé : Elément (mot ou nombre) qui transforme l'application de la méthode de chiffrement et ou déchiffrement.

Classification des codes

Chiffre de substitution : Crypto système dans lequel chaque lettre du message est remplacée par un autre caractère, mais garde sa place dans le message.

Chiffre de transposition : Crypto système dans lequel chaque lettre du message reste inchangée, mais mise à une autre place dans le message.

Substitution mono alphabétique : Chiffre de substitution où l'alphabet chiffré reste le même au cours de tout le chiffrement. Substitution par les lettres, par des symboles, par des chiffres ou nombres...

Substitution poly alphabétique : Chiffre de substitution où l'alphabet chiffré change au cours du chiffrement. Ce changement s'exécute selon une clé.

Code nomenclature : Ce type de chiffre mêle la substitution simple (chaque lettre est remplacée par un symbole) et un code répertoire (certains mots sont remplacés par un symbole également, ainsi que des symboles perturbateurs).

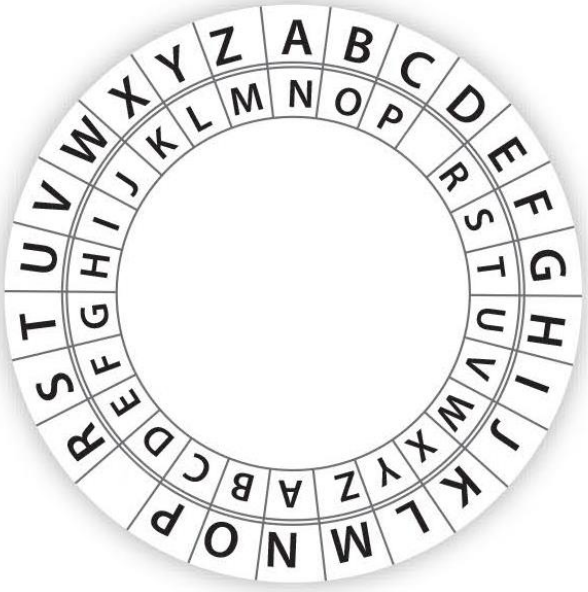
Étape 2 : Activités à faire en classe

Exemple de systèmes de codage les plus connus

1. Le chiffrement de César ou code César

César, pour ses communications importantes à son armée, cryptait ses messages. Ce que l'on appelle le chiffrement de César (substitution mono-alphabétique) est un décalage des lettres de rang 4 : pour crypter un message, **A devient D, B devient E, C devient F,...**

Pour prendre en compte toutes les lettres de l'alphabet, il est plus judicieux de représenter l'alphabet sur une roue.



Crédit Fermat Science

Pour déchiffrer le message

DOHD MDFWD HVW

il suffit donc de décaler les lettres dans l'autre sens, D se déchiffre en A, E en B,...

Le message déchiffré est alors :

ALEA JACTA EST

Déchiffrez les 3 messages suivants :

OHV URPDLQV

YLFWRLUH

HPSHUHXU

2. Le chiffrement de Vigenère

Le chiffre de Vigenère est un algorithme de subsitution polyalphabétique.

Au lieu de faire correspondre circulairement les lettres, on associe maintenant à chaque lettre une autre lettre (sans ordre fixe ou règle générale).

Par exemple :

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
F	Q	B	M	X	I	T	E	P	A	L	W	H	S	D	O	Z	K	V	G	R	C	N	Y	J	U

Pour crypter le message

ETRE OU NE PAS ETRE TELLE EST LA QUESTION

On regarde la correspondance et on remplace la lettre E par la lettre X, puis la lettre T par la lettre G, puis la lettre R par la lettre K...

Le message crypté est alors :

XGKX DR SX OFV XGKX GXWWX XVG WF ZRXVGPDS

Pour le décrypter, en connaissant les substitutions, on fait l'opération inverse.

Déchiffrez les 3 messages suivants :

WXV HFGEXHFGPZ RXV B XVG IFSGFVGPZRX

ADRXK FCXB WXV BEPIIKXV

RSX FRGKX PMXX MXV HFGEV

3. Le chiffre de Porta

Porta était un physicien Italien et inventeur du premier système littéral à double clef, c'est-à-dire le premier chiffre pour lequel on change d'alphabet à chaque lettre
Ce système poly alphabétique était extrêmement robuste pour l'époque, à tel point que beaucoup considèrent Porta comme le "père de la cryptographie moderne".
Giovanni Della Porta a inventé son système de chiffrement en 1563, et il a été utilisé avec succès pendant trois siècles.

Voici un exemple du tableau de chiffrement Porta :

AB	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
CD	a b c d e f g h i j k l m z n o p q r s t u v w x y
EF	a b c d e f g h i j k l m y z n o p q r s t u v w x
GH	a b c d e f g h i j k l m x y z n o p q r s t u v w
IJ	a b c d e f g h i j k l m w x y z n o p q r s t u v
KL	a b c d e f g h i j k l m v w x y z n o p q r s t u
MN	a b c d e f g h i j k l m u v w x y z n o p q r s t
OP	a b c d e f g h i j k l m t u v w x y z n o p q r s
QR	a b c d e f g h i j k l m s t u v w x y z n o p q r
ST	a b c d e f g h i j k l m r s t u v w x y z n o p q
UV	a b c d e f g h i j k l m q r s t u v w x y z n o p
WX	a b c d e f g h i j k l m p q r s t u v w x y z n o
YZ	a b c d e f g h i j k l m o p q r s t u v w x y z n

Crédit photo – apprendre-en-ligne.net

Pour chiffrer avec un de ces alphabets, on choisit pour remplacer la lettre du texte clair la lettre qui lui fait face dans le tableau. Par exemple, si l'on chiffre avec l'alphabet AB, on substituera a par n, b par o, q par d, etc.

Par exemple, si le mot-clef est **ACIER**, on utilisera successivement les alphabets A, C, I, E, R, A, C, etc. pour chiffrer le message. Si l'on chiffre la phrase "**chiffre de Porta**" avec la clef **ACIER**, on obtiendra :

Clair	c	h	i	f	f	r	e	d	e	p	o	r	t	a
Clef	**A**	**C**	**I**	**E**	**R**	**A**	**C**	**I**	**E**	**R**	**A**	**C**	**I**	**E**
Codé	P	T	R	Q	X	E	Q	Z	P	K	B	F	K	Y

Le chiffre porta est celui qu'a utilisé la reine Marie-Antoinette à modifier et améliorer le chiffre PORTA pour s'en servir lors de ses correspondances. Elle a Notamment ajouté une particularité qui est celle de coder seulement une lettre sur deux.

Étape 3 : Pour aller plus loin et idées d'activités à la maison

Et si vous vous lanciez un défi ? Celui de faire passer des messages codés à vos camarades de classe afin qu'ils les déchiffrent.
Par exemple choisissez une méthode de codage et cryptez votre message, ensuite faites le passer sans donner la méthode utilisée.
Rajouter un peu de suspens en donnant un temps imparti ou bien une récompense.

Vous pouvez également créer vous-même la roue de déchiffrement, elle se trouve facilement sur internet :
https://www.youtube.com/watch?v=k7rAXj29iqg

Matériel nécessaire pour la visite

Les élèves participant à la visite devront disposer d'un crayon, d'une gomme et de papier pour trouver le bon code. Un support d'écriture peut être utile pour un meilleur confort.

VISIT MATH

Cofinancé par
l'Union européenne

Ce projet a été financé avec le soutien de la Commission européenne. Cette publication ne reflète que les opinions de son auteur, et la Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qu'elle contient.

Code du projet : 1-FR01-KA220-SCH-00027771

Pour en savoir plus sur Visit Math, rendez-vous sur le site Web du projet : https://visitmath.eu

FERMAT SCIENCE
Une autre idée des maths

5th High School
Agrinio·Greece

ISTITUTO STATALE "E. MONTALE" PONTEDERA

LogoPsyCom

ZS 31

YuzuPulse