mundaneum

UCL
Université catholique de Louvain

Mons
Capitale culturelle

10.10.2017 - 20.05.2018

Top secret!

#TOPSECRETXPO

2017-2018

Dossier thématique

Ed. resp.: Jean-Paul Deplus, rue des passages 15 7000 Mons

TOP SECRET !

Un monde à décrypter

Exposition au Mundaneum, Mons

10.10.2017 - 20.05.2018

Une exposition organisée par le Mundaneum et l'Université catholique de Louvain
Commissariat scientifique : Jean-Jacques Quisquater
Plus d'infos sur notre site : www.mundaneum.org

Remerciement à nos partenaires et, pour la relecture, à France Bral et Baptiste Coppens.

Nos partenaires pédagogiques

Ils nous soutiennent

Nos partenaires prêteurs et institutionnels

Nos partenaires média

SOMMAIRE

AVANT PROPOS p.4

1.Les thématiques abordées p.5

2. Les compétences concernées p.6

3. Lexique p.8

4. . Les fiches thématiques p.10

1. Les origines : la cryptologie manuelle p.10

2. Evolution des techniques, évolution des codes : la cryptographie mécanique p.12

3. Code ou chiffre ? p.13

4. La Seconde guerre mondiale : la guerre des codes p.15

5. Le chiffrement à l'heure de l'informatique : la cryptologie numérique (et quantique) p.17

6. Les hackers: tous méchants ? p.19

5. Quelques repères chronologiques p.21-24

6.Les ressources en bibliothèque, médiathèque et sur le web p.25-27

7. Les animations proposées p.28

8. Les évènements pour les enseignants et opérateurs associatifs p.30

Informations pratiques p.31

AVANT-PROPOS

L'essor d'Internet et des outils numériques a fait de la sécurité des informations un enjeu important, parfois essentiel. Le chiffrement a donc un rôle de plus en plus grand, mais son histoire ne date pas d'hier. Les plus anciennes traces d'écritures secrètes sont contemporaines de l'invention de l'écriture elle-même !

Cacher l'existence d'un message, le coder, le chiffrer, le déchiffrer : d'un usage d'abord restreint aux sphères militaires et politiques, la cryptologie (science des écritures secrètes) occupe aujourd'hui tous les aspects de notre quotidien.

On constate que l''évolution des techniques et des technologies a engendré une évolution parallèle du chiffrement, lutte éternelle entre la cryptographie (coder, chiffrer, crypter) et la cryptanalyse (décoder, déchiffrer, décrypter). Chaque fois qu'un code ou un algorithme est " cassé ", la course reprend pour en créer un plus puissant, et ainsi de suite.

D'un jeu de scribes égyptiens aux communications de guerre, d'innocents messages amoureux au vote électronique, des balbutiements de l'Internet aux enjeux actuels de cybersécurité : l'exposition " Top secret ! " propose un parcours thématique, historique et ludique dans l'univers du secret !

Vous y découvrirez des machines utilisées pour le cryptage mais aussi les hommes et les femmes qui ont contribué au développement de la discipline au fil des siècles.

Qui dit chiffrer dit déchiffrer : culture de la transgression, hacking, mouvements sociaux amplifiés par la cryptographie seront décodés au cœur du Mundaneum, le " Google de papier ".

BONNE VISITE !

Les équipe du Mundaneum et d'UCL Culture ☺

1. LES THÉMATIQUES ABORDÉES

Chapitre 1- La cryptographie dans les objets du quotidien

“Imaginez une société sans secret, une société où tout se saurait sur tout et tout le monde, l'ultra transparence ?“ La réponse : impossible, la crypto est partout ! Une galerie d'objets pucés ou connectés interpelle dans notre société numérisée. Comment protéger nos informations ?

Chapitre 2- L'histoire pour éclairer le présent

Les temps forts de l'évolution de la cryptologie, retracés par des bulles graphiques formant une ligne du temps thématique, à la fois point de départ et ressource au cours de la visite. Ces temps forts sont remis en contexte politique, scientifique, technologique, économique et social, pour se resituer dans l'Histoire.

Chapitre 3 - Célébrer les pionniers : la Seconde guerre mondiale et la cryptographie devient science !

Si la cryptographie ou écriture secrète a toujours existé, il faudra attendre la Seconde guerre mondiale pour que celle-ci ne devienne véritablement une science. Cette évolution de la cryptologie, et surtout de la cryptanalyse, est due en grande partie au travail mené par les équipes de Bletchley Park, parmi lesquelles de nombreuses femmes, oubliées de l'Histoire.

Chapitre 4 - La culture de la transgression : pirates et “hacktivistes“

Les casseurs de code de la seconde guerre mondiale étaient-ils les premiers “hackers“ de l'Histoire? Une contre-culture s'est développée depuis l'avènement de l'informatique. Quelle est la différence entre un black et un white hacker? Qui sont les Cypher-punks? Que revendiquent les Anonymous? Des lanceurs d'alerte comme Edward Snowden au Printemps arabe : revivez des temps forts de l'histoire du numérique amplifiés grâce aux outils de cryptographie.

Chapitre 5 - La Belgique, laboratoire de cryptographie

“L'emploi de la cryptographie est libre“ (extrait du *Moniteur belge*)
Découvrez la Belgique sous un autre jour : “laboratoire“ pour cryptographes ingénieux ! Vote électronique, carte à puce, cryptage des images Canal+ Belgique, algorithme développé par des chercheurs “noirs-jaunes-rouges“ devenu standard international, ... Sur le terrain de la crypto, la Belgique compte parmi les grands !

Chapitre 6 - Et demain ?

A l'ère du big data et du tout numérisé, de grandes questions se posent pour l'avenir de la confiance numérique. Des usages néfastes ou bénéfiques seront faits de nos données, des informations de l'échelle personnelle à celle des Etats... (R)Evolution du mobile et des réseaux sociaux, vie privée, e-commerce, fintech, “guerre“ de l'information, propriété intellectuelle, cybercriminalité, terrorisme ... Autant de problématiques qui se trouvent de plus en plus au cœur du débat politique et public.

2. LES COMPÉTENCES CONCERNÉES

Mathématiques

Analyser et comprendre un message
Résoudre, raisonner et argumenter
Appliquer et généraliser
Généraliser, structurer et synthétiser

- Traduire une information d'un langage à un autre
- Rassembler des arguments et les organiser en une chaine déductive
- Étendre une règle, un énoncé ou une propriété à un domaine plus large
- Calculer l'ensemble des solutions d'une équation, d'une inéquation
- Organiser une suite d'opérations conduisant à la résolution d'un problème
- Traiter des données : lire et interpréter un tableau, un graphique, un diagramme
- Intégrer le savoir dans une culture scientifique et humaniste

Sciences et initiation scientifique (éveil)

Faire émerger une énigme et la résoudre
Développer la curiosité, l'honnêteté intellectuelle et l'équilibre entre ouverture d'esprit et scepticisme
Participer aux grands débats engendrés par une société scientifico-technique

- Observer de manière divergente en utilisant tous ses sens
- Identifier des indices et dégager des pistes de recherches propres à la situation
- Dans le cadre d'une énigme, agencer les indices en vue de formuler au moins une question, une supposition ou une hypothèse ; proposer une piste de résolution possible
- Évaluer l'impact de découvertes scientifiques et d'innovations technologiques sur notre mode de vie
- Utiliser les raisonnements inductifs, déductifs, par analogie et par analyse systémique

Histoire et formation historique (éveil)

Rechercher de l'information
Communiquer
Faire preuve d'esprit critique
Agir et réagir : s'engager et assumer un engagement

- Utiliser des repères de temps
- Lire une trace du passé et l'interpréter
- Remettre dans son contexte historique, analyser et critiquer un ensemble limité de sources
- Mettre en évidence des permanences, des processus évolutifs, des changements ou des synchronismes
- Prendre une part active à l'élaboration et à la réalisation d'un projet pour promouvoir la justice, la solidarité, le sens des responsabilités vis-à-vis des autres, de l'environnement et du patrimoine

Education à la citoyenneté, morale et cours confessionnels : sujets annexes

Droits de l'Homme
Vie privée
Informatique
Journalisme
Piratage, hacking
Lanceurs d'alerte
Moyens de communication
Langage
Égalité homme-femme
Droits des minorités
....

3. LE LEXIQUE

Cryptologie : science de l'écriture secrète, englobant la cryptanalyse et la cryptographie.

Cryptanalyse : technique qui permet de déduire le texte en clair à partir du texte chiffré, sans connaître la clé.

Cryptographie : technique de chiffrement d'un message, ou ensemble des méthodes utilisées pour cacher le sens d'un message.

Stéganographie : technique pour cacher l'existence d'un message, par opposition à la cryptographie qui en dissimule le sens.

Code : système pour dissimuler le sens d'un message en remplaçant chaque mot ou phrase par un caractère ou un ensemble de caractères différents.

Crypter : chiffrer ou coder.

Chiffrer : transformer le message d'origine en message chiffré.

Déchiffrer : transformer un message chiffré en un message clair, conforme à l'original, soit en utilisant la clé, soit en utilisant la cryptanalyse.

Décoder : transformer un message codé en message clair conforme à l'original.

Décrypter : déchiffrer ou décoder.

Texte clair : message original avant chiffrement.

Texte chiffré : message obtenu après chiffrement.

Chiffre : n'importe quel système appliqué pour dissimuler le sens d'un message en remplaçant chaque lettre du message d'origine par une autre.

Chiffre par substitution : système dans lequel chaque lettre est remplacée par un autre caractère mais garde sa place dans le message. Il peut être monoalphabétique (l'alphabet chiffré reste le même pour tout le message) ou polyalphabétique (l'alphabet chiffré change au cours du déchiffrement).

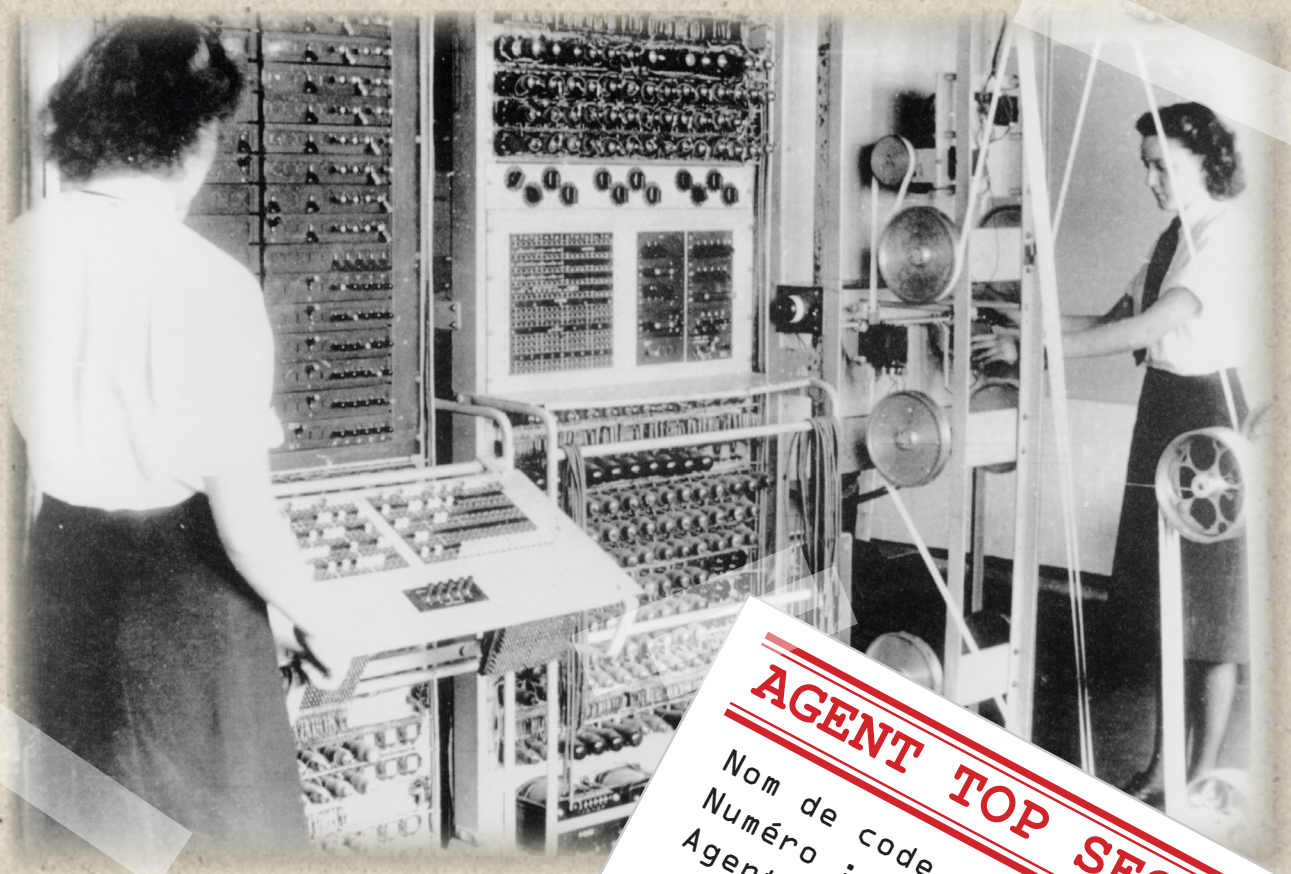
Chiffre par transposition : système dans lequel chaque lettre reste inchangée mais mise à une autre place dans le message.

Clé : paramètre qui transforme l'application de l'algorithme de chiffrement en le spécifiant.

Algorithme de chiffrement : suite d'opérations à effectuer pour le chiffrement, liée à une clé qui le précise.

Clé privée / clé publique : L'envoyeur utilise une clé publique pour crypter les messages. Le receveur utilise une clé privée, qui doit rester secrète, pour décrypter les messages.

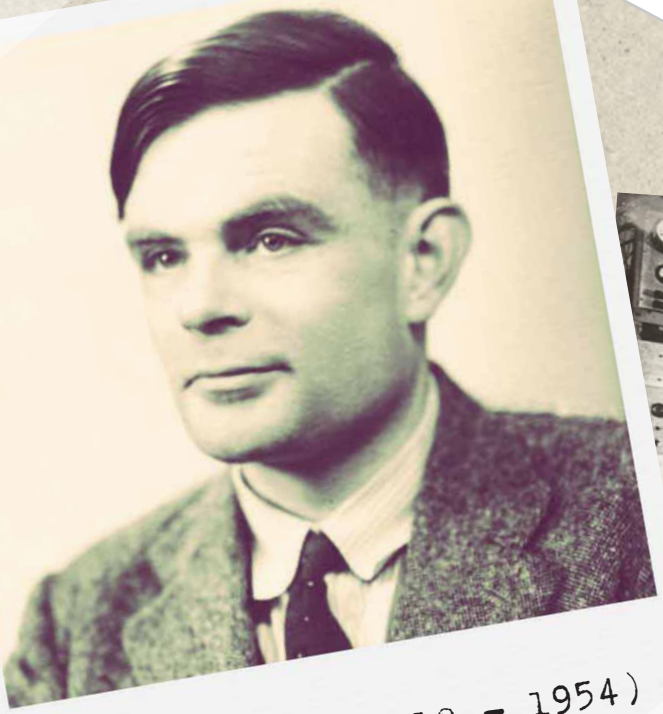
Ordinateur quantique : ordinateur extrêmement puissant qui applique la théorie quantique, en particulier la théorie disant que chaque objet peut être dans tous les états à la fois ou qu'un objet peut être dans plusieurs univers en même temps.



Bletchley Park

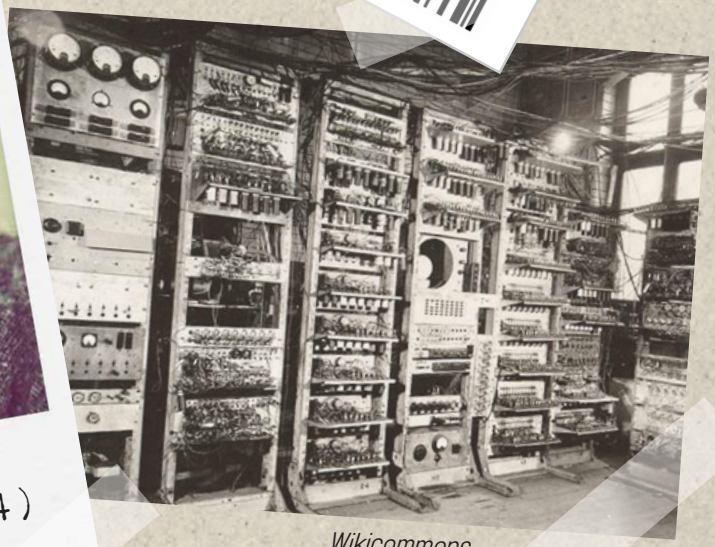
AGENT TOP SECRET

Nom de code :
Numéro :
Agent depuis le : 10.10.17
Délivré au Mundaneum



Alan Turing (1912 - 1954)

King's College Cambridge



Wikicommons

4. LES FICHES THÉMATIQUES

1. Les origines : la cryptologie manuelle

HISTOIRE – LANGUES – MATHEMATIQUES

Les plus anciens chiffrements connus sont les hiéroglyphes égyptiens, qui datent d'environ 3000 ans avant notre ère. Longtemps oublié, cet alphabet est traduit au XIXe siècle par Jean-François Champollion grâce à la découverte de la pierre de Rosette.

Dans l'Antiquité déjà, diverses méthodes apparaissent pour cacher des messages. L'une des premières méthodes est le " **chiffrement par transposition** " : il consiste à changer l'ordre des lettres. À Sparte, en Grèce, au VIe siècle, on invente ainsi la scytale, un bâton autour duquel l'expéditeur enroulait une bandelette pour y écrire son message. Seule la bandelette était envoyée au destinataire. Si cette personne possédait un bâton d'un même diamètre, elle pouvait alors enrouler la bande autour de celui-ci afin de lire le message original.

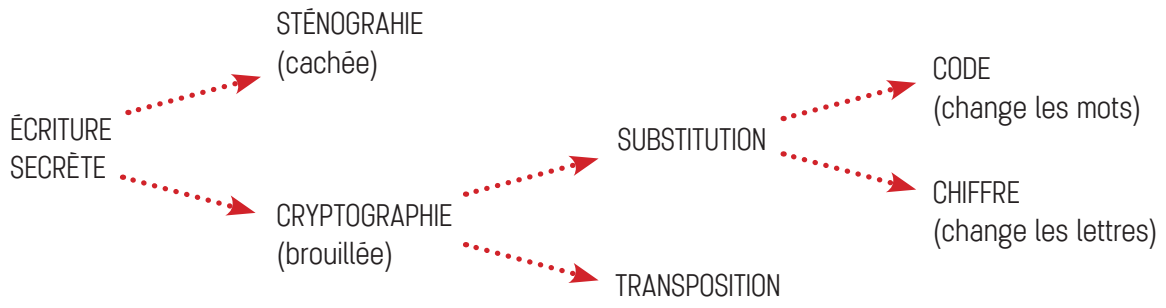
Autre méthode, le " **chiffrement par substitution** " comme le célèbre " chiffre de César ", du nom du général romain (Ier siècle avant notre ère). Il remplace chaque lettre du message par une autre située à une distance fixe dans l'alphabet. La clé pour le déchiffrer : connaître le décalage. Mais une lettre remplace toujours la même lettre dans le message. Un autre exemple est le " carré de Polybe " : le mathématicien et historien grec Polybe (IIe siècle avant notre ère) a créé une grille où chaque lettre est représentée par la combinaison du chiffre de sa ligne et du chiffre de sa colonne.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Une technique pour déchiffrer ce type de message chiffré par substitution a été découverte par les mathématiciens arabes, qui inventèrent ainsi la cryptanalyse au IXe siècle : l'analyse de fréquences. Le principe repose sur la répétition de certaines lettres ou mots pour une langue précise. Par exemple, en français, le "e" est la lettre la plus souvent utilisée; "q" est presque toujours suivi par "u"; les mots "un", "une", "le", "la", "les", "des" apparaissent aussi très souvent.

Une réponse à cette méthode efficace de cryptanalyse est apparue au Moyen Âge : le chiffrement polyalphabétique, par exemple le chiffre de Vigenère. Il croise 26 variations de l'alphabet. Un mot clé, connu de l'expéditeur et du destinataire, permet de savoir quelle ligne alphabétique utiliser et dans quel ordre. Cette méthode fiable de chiffrement ne sera " cassée " qu'avec l'apparition des machines à calculer au XIXe siècle !

Une autre méthode est appelée la stéganographie. Elle vise non pas à brouiller le message, mais à le cacher tout simplement : encre sympathique, image trafiquée, ou encore phrase anodine qui a un sens secret pour l'expéditeur et le destinataire (comme les messages de la Résistance française durant la Seconde guerre mondiale).



Pour aller plus loin : Testons nos méninges et cassons les codes !

Pour mieux comprendre cette thématique, l'idéal est de tester le chiffrement et le déchiffrement de différents codes. La difficulté peut être adaptée en fonction du groupe. Voici quelques exemples.

1. Carré de Polybe

13 – 34 – 14 – 15 : _ _ _ _
ZIGZAG : _ _ _ _ _ _

2. Chiffre de César

Pour rappel: A=D; B=E; C=F; ...
CESAR : _ _ _ _ _
KRWHO : _ _ _ _ _

3. Analyse de fréquence

YRF RYRIRF QR PRGGR PYNFFR FBAG SBEGFRA ZNGURZNGVDHRF

_ _

Marche à suivre : Compléter le tableau suivant puis comparer la fréquence d'apparition des lettres dans ce texte (l'ordre de fréquence plutôt que le pourcentage) avec la fréquence théorique d'apparition des lettres d'un texte de la langue française. En déduire le décryptage du texte en faisant attention aux déterminants courants et aux lettres doublées.

Lettre	A	B	C	D	E	F	G	H	I
Nombre									
Fréquence									
Lettre en clair									

Lettre	J	K	L	M	N	O	P	Q	R
Nombre									
Fréquence									
Lettre en clair									

Lettre	S	T	U	V	W	X	Y	Z	
Nombre									
Fréquence									
Lettre en clair									

E	17,52
S	8,17
A	8,01
I	7,35
N	7,22
T	7,07
R	6,69
U	6
L	5,77
O	5,43
D	3,91
C	3,23
P	2,94
M	2,90
V	1,41
Q	1,14
G	1,06
F	1,06
H	0,88
B	0,88
X	0,47
J	0,44
Y	0,30
Z	0,12
K	0,05
W	0,02

Fréquence théorique des lettres en français (en%)
https://www.apprendre-en-ligne.net/crypto/stat/francais.html

SOLUTIONS
1. CODE – 55-24-22-55-11-22
2. FHVDU – HOTEL
3. Les élèves de cette classe sont fort en mathématiques. *Code : A=N, N=A*

2. Evolution des techniques, évolution des codes : la cryptographie mécanique

HISTOIRE – SCIENCES – TECHNOLOGIE

Pendant plusieurs siècles en Occident, les codes vont peu évoluer. D'une part parce que l'usage de chiffres polyalphabétiques efficaces se répand, d'autre part parce que les chefs militaires et politiques préfèrent " cacher " les messages (dans des objets, sur des vêtements, etc.) plutôt que les chiffrer de manière complexe. Cela laisse la place libre aux espions de toutes sortes... jusqu'à la Révolution française.

Claude Chappe (FR, 1763-1805) utilise les avancées technologiques de son époques en mécanique* et en optique* pour créer un **télégraphe optique et manuel**. Un télégraphe est un système destiné à transmettre des messages, appelés télégrammes, d'un point à un autre sur de grandes distances, à l'aide de codes pour une transmission rapide et fiable.

Celui imaginé par Chappe est composé d'un grand mât et de trois planches formant des bras articulés visibles jusqu'à 10 km. Un système de relais permet de faire parcourir de très longues distances à un message, en quelques instants, alors que jusqu'ici il fallait un envoi (coursier à cheval, pigeon voyageur...). Chappe imagine donc aussi un code alphabétique utilisant la position des bras de son télégraphe, qui doit rester confidentiel afin que tout le monde ne puisse pas comprendre les messages.

Un système similaire est le **sémaphore** développé pour la marine, qui utilise des drapeaux colorés et des gestes précis des bras pour transmettre les messages à distance.

Quelques décennies plus tard, **Samuel Morse** (US, 1791-1872) utilise lui aussi le système du télégraphe, mais tire parti de l'électricité récemment découverte : des signaux intermittents, courts ou longs, sont associés pour former des lettres ou des chiffres. Le **code Morse** n'est pas fait pour rester secret, mais seuls ceux qui le connaissent peuvent décoder les messages. Le système devient universel car c'est un moyen rapide, économique et simple de transmettre des messages un peu partout dans le monde. L'alphabet ou code Morse peut être utilisé pour transmettre un texte à l'aide de signaux visuels (gestes, lumière) ou sonore.

En facilitant la communication et les transports, le télégraphe électrique et le chemin de fer seront les éléments déterminants de la Révolution industrielle en Europe et aux Etats-Unis.

C'est finalement l'invention de la **radiotélégraphie** (la radio), aussi appelée TSF (télégraphie sans fil), par Guglielmo Marconi en 1894 qui rend l'évolution du chiffrement nécessaire : une fois que tous utilisent la radio pour communiquer, tout le monde peut intercepter les messages ! Le besoin devient très urgent lorsqu'éclate la Première guerre mondiale. C'est d'ailleurs grâce au déchiffrement par les Anglais d'un télégramme de l'ambassadeur allemand que les Etats-Unis, menacés sur leur territoire, acceptent d'entrer en guerre. Il faut cependant attendre 1918 pour qu'un chiffre efficace soit créé par les Allemands... qui sera lui aussi déchiffré en quelques mois seulement par les Français.

Tout cela explique pourquoi, une fois la guerre finie, ce sont les Allemands qui s'intéresseront à la mécanisation du codage.

Quelles inventions ou nouveaux outils changent la manière de communiquer de nos jours ?

* **Mécanique** : la science des machines.

* **Optique** : la science qui étudie les phénomènes liés à la lumière et à la vision.

Pour aller plus loin : construire un télégraphe Morse

http://www.cndp.fr/crdp-rennes/crdp/crdp_dossiers/dossiers/goutdefil/prattele.htm
https://www.ac-strasbourg.fr/fileadmin/pedagogie/physiquechimie/college/college_2016/Communiquer_en_temps_de_guerre.pdf

3. Code ou chiffre ?

FRANÇAIS – HISTOIRE

Il existe des codes qui n'ont pas été conçu pour rester secrets, mais qui le sont car tout le monde ne les apprend pas. C'était le cas avec le **code Morse** (**page 12**), c'est aussi le cas, par exemple, de **l'écriture Braille**. Louis Braille (1809-1852) s'inspire d'une " écriture nocturne " conçue par l'armée française pour être lue sans lumière. Braille n'a que 15 ans lorsqu'il améliore le système pour en faire une véritable écriture, qui permet aussi de noter les mathématiques et la musique ! Son système utilise des points pouvant occuper 6 positions réparties en 2 colonnes. Chaque caractère est donc formé d'une combinaison de 1 à 6 points.

Parfois, c'est justement parce qu'une **langue existante** est parlée par un petit nombre de gens seulement, qu'elle fait un très bon code secret ! Les Etats-Unis ont compris cela et ont fait appel, durant les deux guerres mondiales, à des **" code-talkers " ou " parleurs de code "**, en fait des soldats Amérindiens, comme les Navajos. Pourquoi étaient-ils si efficaces? Parce qu'ils ne chiffraient pas les messages, mais les traduisaient simplement dans leur langue. Les ennemis ne la connaissaient pas, car elle ne ressemblait à aucune autre langue et n'avait pas été étudiée ou traduite à l'époque. Ils devaient seulement trouver des symboles pour représenter les avions (différents oiseaux pour différents modèles) ou les bateaux et sous-marins (poissons), qui n'existaient pas dans la langue traditionnelle. Il reste un des rares codes à n'avoir jamais été cassé !

Langue – Code – Chiffre : quelle différence ?

Une **langue** est un système composés de signes vocaux (voix, clic de la langue), graphiques (écriture, dessin) ou gestuels, qui permet la **communication** entre les individus. Ce système peut évoluer avec le temps ou en fonction des régions géographiques où la langue est utilisée.

Toute communication repose sur différents éléments :

- *Le contexte*: ce à quoi on se réfère
- *Le message*: l'information essentielle
- *Le destinateur / émetteur* : celui qui envoie le message
- *Le destinataire / récepteur*: celui qui reçoit le message
- *Le canal*: le moyen par lequel on transmet le message (oralement, sur papier, par la radio,...)
- *Le code*: la formulation du message sous une forme compréhensible pour le destinataire

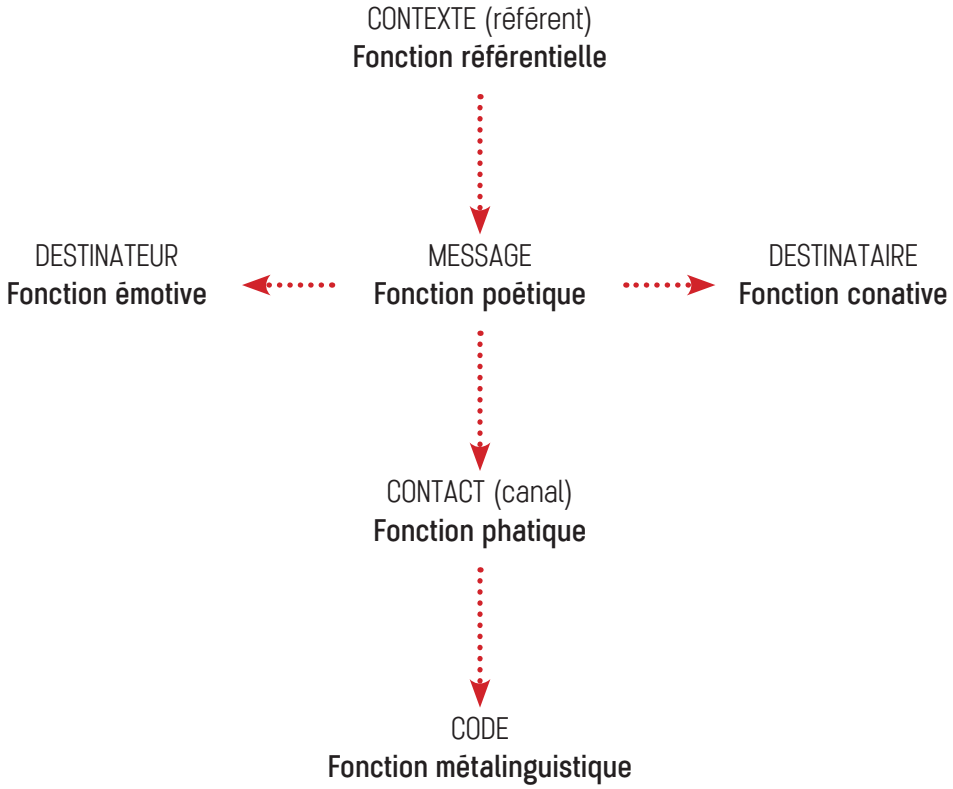
Un **code** est donc simplement un moyen de communiquer partagé entre l'émetteur et le récepteur, qui permet de diffuser l'information et de gagner du temps. Le codage transforme de l'information en un ensemble de mots, de symboles : l'écriture est un code, une langue parlée est un code, le Morse est un code,...

À l'inverse, un **chiffrement** sert à protéger, cacher l'information, et à empêcher des personnes autres que le récepteur prévu d'y accéder. Les chiffrements ne concernent pas la signification du message lui-même : ce sont des opérations appliquées dans un certain ordre (donc des **algorithmes**) à une ou plusieurs composants du message (lettre, nombre, mot, etc.).

En cryptographie, le code travaille sur la signification, le sens des mots ou des phrases, tandis que le chiffrement travaille sur les composants élémentaires du message, comme les lettres ou les bits. Par exemple, l'utilisation des noms de poissons pour les bateaux par les soldats Navajo est un code, tandis que le mélange des lettres dans une phrase est un chiffrement

Pour aller plus loin

Schéma de la communication de Roman Jakobson (1963), version simplifiée.
Source http://www.linguistes.com/langue/intro.htm



Selon l'axe choisi, l'analyse individuelle et/ou en groupe des éléments constitutifs de la communication, pour un message donné (texte, image, audiovisuel), permettra aux élèves de :

- s'approprier le schéma de communication et d'expliquer les systèmes de codage et de décodage de l'information ;
- différencier une observation d'un jugement et d'une interprétation ;
- produire un message structuré qui exprime un avis, une prise de position devant un fait, un événement, ...
- prendre conscience des enjeux de la communication interpersonnelle et de l'importance du langage verbal et non verbal ;
- réfléchir par rapport à son propre fonctionnement relationnel ;
- analyser les critères permettant de développer une communication efficace et les justifier.

Il existe des leçons disponibles en ligne, par exemple, pour le secondaire :
www.enseignons.be/secondaire/preparations/le-schema-de-communication/

4. La Seconde guerre mondiale : la guerre des codes

HISTOIRE - TECHNOLOGIE

Avec leur défaite en 1918, les Allemands prennent conscience de l'importance d'un chiffrement efficace de leurs communications. L'essor des machines cryptographiques culmine pour un temps avec l'invention de l'Enigma par Arthur Scherbius.

La **machine Enigma** intègre une méthode de chiffrement par substitution polyalphabétique automatisée. La machine est composée de rotors (d'abord 3 puis 5) numérotés de 1 à 26 pour les lettres de l'alphabet, d'un dispositif appelé "réflecteur" ou "brouilleur", et d'un tableau de connexion câblé permettant une première conversion monoalphabétique. Les lettres du texte clair sont tapées sur le cadran, la lettre chiffrée s'éclaire. Mais le rotor de droite tourne d'un cran à chaque frappe, le 2e toutes les 26 frappes, le 3e toutes les 676 frappes (26^2), et ainsi de suite, ce qui veut dire qu'une lettre en clair allume à chaque frappe une lettre chiffrée différente. Tout cela est quasi instantané, chiffrer le texte prend tout juste un peu plus de temps que le taper à la machine !

La force de l'Enigma est que les réglages étaient changés chaque jour : ordre et orientation initiale des des rotors, et branchement des câbles du tableau de connexion. Un exemple de clé :

- Position des rotors : 3 – 4 – 1 – 5 – 2
- Orientation des rotors : 7 – 20 – 12 – 3 – 25
- Connexions : A=D – T=X – I=F – C=V – O=Y

Sans connaître ces réglages, la machine ne sert à rien à celui qui essaie de déchiffrer le message.

Alors que la majorité de l'Europe ne s'intéresse pas à ce nouvel outil des Allemands, la Pologne, qui se sent alors menacée d'invasion par son grand voisin, entreprend de décrypter le code Enigma. Les cryptanalystes polonais y parviennent presque, inventant une "bombe" cryptologique (machine à calculer), mais ils doivent abandonner faute de moyens. En été 1939, les Polonais transmettent en secret leurs travaux et deux machines Enigma à la Grande-Bretagne. Deux semaines plus tard, l'Allemagne nazie envahit la Pologne et déclenche ainsi la Seconde guerre mondiale...

Les services secrets britanniques reprennent les travaux des Polonais et les perfectionnent, jusqu'à l'invention de la fameuse "bombe logique de Turing" à Bletchley Park, près de Londres. Cette machine à calculer électromécanique, inspirée de la machine polonaise et perfectionnée par le mathématicien Alan Turing, permet de décrypter les messages de l'Enigma sans connaître la clé du jour. Un exploit classé "secret défense" jusque dans les années 1970.

Durant la guerre, Les Britanniques développeront aussi le calculateur Colossus, et les Américains l'ENIAC (Electronic Numerical Integrator And Calculator) : ces deux machines sont le point de départ de l'informatique !

La cryptographie mécanique ne met pourtant pas un terme aux vieilles méthodes : la Résistance française communique depuis Londres grâce à des **messages stéganographiques**. Les célèbres messages de ***Radio Londres***, "Les Français parlent aux Français", sont incompréhensibles pour ceux qui ne font pas partie du réseau de Résistants. Une phrase anodine comme "Attention à l'œuf dans l'omelette" ou "Amédée déteste le vinaigre" avait une signification cachée qui pouvait annoncer un parachutage, une trahison, une opération en cours, etc. Le plus connu des messages est tiré d'un poème de Verlaine : "Les sanglots longs des violons de l'automne blessent mon cœur d'une langueur monotone". Il annonçait le Débarquement des armées alliées en Normandie...

La Seconde guerre mondiale a donc été marquée par les avancées des cryptographes et des cryptanalystes, qui, en parallèle aux grandes batailles sur terre, sur mer et dans les airs, se sont livrés une guerre sans merci !

Pour aller plus loin

1. Construire sa propre Enigma avec un tube en carton

Instructions et exemples sur le site web (en anglais) : Franklin Heath, Paper Enigma
http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma

Préparation :

- Aligne les lignes grises sur le réflecteur et sur le cylindre d'entrée / sortie (Input / Output) Cela montre la position de départ de ta machine Enigma et te permet de vérifier les rotations.

- Tourne les rotors pour que les trois lettres de ta clé de message (pour cet exemple ABC) soient alignés avec les barres grises : rotor I=A ; rotor II=B ; rotor III=C

Pour chaque lettre de ton message:

- Tourne seulement le rotor III (à droite) d'un cran vers toi, de sorte que la lettre en face de la barre grise devient la suivante selon l'ordre alphabétique. Vérifie que les autres rotors et le cylindre d'entrée / sortie ne bougent pas.
  Tu dois le faire avant même de lire la première lettre !

- Trouve la lettre de ton message sur le cylindre d'entrée / sortie (le plus à droite) et suit la ligne à travers les trois rotors, dans le réflecteur, reviens à nouveau dans les trois rotors et finalement dans le cylindre d'entrée / sortie à nouveau.
  Note la lettre, puis recommence pour les suivantes : tourner le rotor III d'un cran, suivre la ligne, etc.

Essaie avec ce message:

W M T M L

Sur une vraie machine Enigma, quand le rotor de droite tourne un certain nombre de fois, d'autres rotors tournent aussi, ce qui rend le mélange des lettres plus difficile à prédire.
Lis bien ces instructions !

2. Une liste des messages diffusés par *Radio Londres*

http://www.messages-personnels-bbc-39-45.fr/

5. Le chiffrement à l'heure de l'informatique : la cryptologie numérique (et quantique)

HISTOIRE – MATHEMATIQUES

Après la Seconde guerre mondiale et la construction des premiers ordinateurs, le cryptage et le décryptage des messages évoluent **du mécanique vers le numérique**. La cryptographie, qui était depuis des siècles l'affaire de linguistes passionnés de mots et de combinaisons de lettres, devient celle des mathématiciens et des informaticiens.

La cryptologie, auparavant réservée aux domaines militaire et politique, devient aussi un enjeu pour la sphère **civile et publique** : comment protéger les opérations commerciales ou bancaires, qu'elles soient téléphoniques ou informatiques ? Comment envoyer des courriers électroniques sans que tout le monde puisse les lire ? Il faut sécuriser les informations qui circulent en créant des systèmes algorithmiques mathématiques de chiffrement, c'est-à-dire des opérations de cryptage effectuées successivement et dans un ordre préétabli de manière automatique par ordinateur. Le Bureau des Standards américain (NBS puis NIST) lance donc dans les années 1970 un appel d'offre pour un tel système, que tout le monde pourrait utiliser.

Clé privée / clé publique

C'est d'abord le DES (Data Encryption Standard) qui est mis en place. Il s'agit d'un système de chiffrement symétrique: une seule clé secrète est la même pour le cryptage et le décryptage. Son fonctionnement est suffisamment complexe pour chiffrer les messages dans cette période où l'informatique se développe. L'algorithme consiste à traduire le message en nombre binaire (bits), puis à le diviser en blocs de 64 bits qui sont mélangés. On divise ces blocs mélangés en deux blocs de 32 bits qu'on remélange, et on répète l'opération 16 fois. C'est comparable à de la pâte feuilletée qu'on découperait en bandes de 64 cm avant de la diviser, la pétrir, la replier, la mélanger à nouveau pour former une nouvelle bande, et on recommence tout. Mais ce système a un défaut : la distribution de la clé entre émetteur et récepteur du message.

Plusieurs mathématiciens trouveront la solution, plus ou moins au même moment : le principe de clé privée / clé publique, ou système de chiffrement asymétrique. L'émetteur et le récepteur utilise chacun une clé pour chiffrer et déchiffrer, clé qui n'est pas identique. L'algorithme utilise, pour créer la clé, des fonctions mathématiques complexes, comme l'arithmétique modulaire ou la factorisation des nombres premiers.

En termes simples, on peut imaginer que :

- Alice veut envoyer un message à Bob sans que personne ne puisse le comprendre.
- Alice place le message dans la boîte, la ferme avec son cadenas et l'envoie à Bob.
- Bob ajoute son propre cadenas, puis renvoie la boîte à Alice.
- Alice retire alors son cadenas et renvoie la boîte à Bob, qui n'a plus qu'à retirer son cadenas pour ouvrir la boîte.

L'algorithme RSA (des initiales de ses inventeurs) fonctionne sur ce principe. Il protège la majorité des échanges d'information sur Internet aujourd'hui. La question de la sécurité se pose à l'heure actuelle pour les smartphones et objets connectés... et bientôt pour les ordinateurs quantiques.

Les ordinateurs quantiques : le futur du (dé)chiffrement

Puisqu'il est impossibles aux ordinateurs actuels de calculer rapidement les factorisations nécessaires au décryptage du RSA, les cryptologues se tournent vers l'avenir de l'informatique : les ordinateurs quantiques. Leur principe repose sur la théorie quantique en physique, qui postule qu'un élément (quantum) peut soit occuper tous

les états simultanément (superposition d'états), soit occuper un état défini dans une multitude d'univers (états parallèles). Le résultat est le même : une infinité d'états, qui se traduit pour notre ordinateur en une infinité de calculs effectués simultanément. En cryptographie, cela se traduira par une transmission de message que seul le destinataire véritable pourra comprendre, puisque lui seul aura la clé pour savoir quelles valeurs aléatoires sont les bonnes. Ce système permettra en outre de savoir si quelqu'un tente d'intercepter le message, car chaque quantum serait perturbé par cette intervention. L'informatique quantique offre donc la perspective d'une cryptographie incassable !

Pour aller plus loin : La cryptographie à clé publique et l'algorithme RSA

Source : *Histoire du chiffrement et de ses méthodes. Synthèse chronologique du chiffrement à travers les âges*, Thawte, 2013, p. 10-11.[1]

Le concept d'échange de clés Diffie-Hellman-Merkle utilise l'arithmétique modulaire Y=AX(mod B), une arithmétique dite « à sens unique » du fait de la difficulté pratique à inverser l'exponentiation modulaire. Un calcul à l'aide de la méthode suivante, qui utilise la fonction selon laquelle AX divisé par B donne Y, a la particularité étonnante d'offrir le même résultat. C'est selon ce principe que la cryptographie à clés communes a pu évoluer.

- L'expéditeur et le destinataire partagent déjà A et B (par exemple, A=7 et B=11).
- X correspond à une valeur que les deux parties connaissent mais ne partagent pas (par exemple, X=3 et x=6).
- Les valeurs respectives de Y sont déterminées à partir de celles de A et B, partagées, et des valeurs respectives de X (ainsi Y=2 et y=4).
- L'expéditeur et le destinataire partagent alors leurs valeurs respectives de Y.
- Ils recalculent enfin la solution par arithmétique modulaire, à l'aide de leurs propres X respectifs et du Y de leur interlocuteur. Résultat : (Yx(mod 11) = 26(mod 11) = 9, yX(mod 11) = 43(mod 11) = 9

Selon cette méthode, il est possible de mener une conversation confidentielle sur une place publique. (...)
L'algorithme RSA (Rivest-Shamir-Adleman) repose lui sur la factorisation d'un nombre donné en produit de nombres premiers (nombres divisibles uniquement par eux-mêmes et par 1), comme le montre l'exemple ci-dessous.

- 95=5 × 19
- 851=23 × 37
- 176653=241 × 733
- 9831779=2011 × 4889

Dans le cadre de la cryptographie à clé publique, le nombre situé à gauche de l'équation sert de clé publique et fait partie de la clé privée. Si le nombre premier est un très grand nombre entier, il devient très difficile de décrypter le nombre premier à droite de l'équation dans un délai raisonnable par factorisation première.

Une animation mathématique "Introduction à la cryptographie et au système RSA" a été conçu pour les élèves du secondaire par ScienceInfuse (UCL). Les dossiers élève et prof sont disponibles sur demande à info@mundaneum.be.

[1] https://www.thawte.fr/assets/documents/guides/history-cryptography.pdf, consulté le 01.06.2017

6. Les hackers: tous méchants ?

PHILOSOPHIE – EDUCATION À LA CITOYENNETÉ

" *To hack*" en anglais signifie "découper" quelque chose, c'est-à-dire : décomposer pour recomposer, bidouiller, bricoler. Les **pirates informatiques**, en anglais "*hackers*", se décrivent comme des chapeaux blancs ou noirs, comme les **gentils ou méchants** cowboys au cinéma.

- "Chapeau noir" : Pirate informatique qui pénètre les systèmes informatiques avec une intention criminelle.
- "Chapeau blanc" : Pirate qui pénètre dans un système informatique à la demande de son propriétaire, pour mieux le sécuriser.
- "Chapeau gris" : Pirate qui entre sans y être autorisé dans les systèmes mais ne veut pas commettre de crime. Il veut aider le propriétaire, dénoncer un crime ou simplement réaliser un "exploit" informatique !

Les différentes couches du web

Il existe une partie du web (le réseau Internet) inconnue du grand public. Le web a en fait différentes "couches":

- Le web de surface **ou web visible** est la partie du web accessible à tous et consultable par les moteurs de recherche.
- Le **web profond** ou invisible est la partie du web qui n'est pas consultable directement par les moteurs de recherche: seuls les utilisateurs ayant les codes d'accès peuvent les consulter.
- Le *dark web*, dark net ou **le web de l'ombre,** est la partie la plus cachée du web invisible. Parce qu'il est chiffré, l'anonymat y est garanti pour les utilisateurs, les hébergeurs, et les détenteurs de ressources web.

Si les principales raisons d'utilisation du dark web ont de quoi effrayer (pornographie infantile, trafic de drogues ou d'armes), celui-ci peut aussi servir des intérêts positifs. Il permet à des dissidents politiques* vivant sous des régimes totalitaires ou des lanceurs d'alerte* de relayer leurs idées sans crainte de représailles, et il est utilisé par de nombreux journalistes pour protéger leurs sources confidentielles.

Quelques exemples réels d'utilisation de systèmes chiffrés (e-mails, publications) utilisés à des fins "éthiques":

- La propagation des idées et l'organisation de manifestations lors des "Printemps arabes", c'est-à-dire des mouvements populaires en faveur de la démocratie dans de nombreux pays arabes entre 2010 et 2014.
- En Chine, de nombreux dissidents politiques diffusent des articles plaidant pour une démocratisation du régime sur leurs blogs ou par courrier électronique cryptés.
- L'*hacktivisme* ou **cyberactivisme** est une forme numérique de désobéissance civile*: les piratages, détournements de serveurs, diffusion de données confidentielles sont utilisés comme moyen non-violent de protestation en faveur de la liberté d'expression. Ces pratiques sont parfois considérées comme criminelles par les gouvernements, comme celles du groupe Anonymous.*
-

* **Dissident politique**: Le dissident n'est plus d'accord avec l'autorité à laquelle il devait se soumettre jusqu'alors, et conteste de façon plus ou moins forte le système politique du pays où il vit.

* **Lanceur d'alerte**: personne, groupe ou association qui prévient d'un danger ou d'un risque. En lançant l'alerte, on court soi-même un danger (perte de son emploi, procès ou autre) et on devient donc une personne à protéger.

* **Désobéissance civile** : refus annoncé publiquement d'obéir à une loi ou un règlement parce qu'on le trouve injuste et contraire à ses valeurs. C'est une manière pacifique, non-violente de protester.

* **Anonymous** (en français : les "Anonymes") est un groupe mondial de pirates informatiques qui réalisent des attaques afin de défendre la liberté d'expression. Ils manifestent parfois dans la rue et portent alors un masque pour ne pas être reconnus.

Pour aller plus loin : quelques questions à débattre

- Y a-t-il de bonnes ou de mauvaises raisons de désobéir à la loi ?
- Un « pirate informatique » est-il forcément un criminel ?
- Est-ce logique de dire qu'on défend la loi, mais l'enfreindre soi-même ? Et dire qu'on défend la liberté, mais empiéter sur la liberté ou la vie privée d'autres personnes, est-ce logique ?
- Un système informatique, comme le dark web, qui permet de commettre des crimes mais pas seulement : faut-il l'interdire ou l'autoriser ?
- Les lanceurs d'alerte, Wikileaks, Anonymous : est-ce la même démarche ? Qui faut-il protéger ?
- Le secret est-il bon ou mauvais ?
- Devrait-on savoir tout sur tout le monde ? Que doit savoir le public des secrets de fabrications des entreprises, des plans de centrales nucléaires, des déplacements des hommes politiques, etc. ?

En primaire :

Dossier pédagogique, Être citoyen, c'est quoi ?, Phileas et Autobule, n°51

http://www.phileasetautobule.be/Dossier-pedagogique-du-N-51-Etre-citoyen-c-est-quoi_a921.html

En secondaire :

Henry David Thoreau (1817-1862, USA), La désobéissance civile, Passager Clandestin, 2007, 75 pages.

Documentaire : Les nouveaux désobéissants, un film d'Arthur Borgnis (FR, 52 minutes)

http://www.lcp.fr/emissions/droit-de-suite/151402-les-nouveaux-desobeissants

5. QUELQUES REPÈRES CHRONOLOGIQUES

– 400 Scytale

Inventée par les Spartiates durant l'Antiquité, la scytale était un bâton de bois utilisé pour lire ou écrire un message chiffré. Le message écrit sur une bandelette doit être enroulé sur un bâton de la bonne circonférence.

Wikicommons

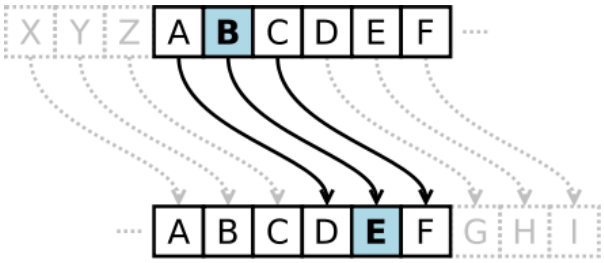
– 150 Carré de Polybe

Le mathématicien, historien et écrivain grec Polybe (vers 150 avant notre ère) a créé une grille de chiffrement par substitution. Chaque lettre est représentée par la combinaison du chiffre de sa ligne et du chiffre de sa colonne (exemple : A=11, B=12). Cette méthode a été utilisée par plusieurs civilisations de différentes manières tout au long de l'histoire.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

– 50 Chiffre de César

Le général romain Jules César (Ier siècle avant notre ère) codait ses messages en remplaçant chaque lettre par celle qui se situe 3 places plus loin dans l'alphabet. On peut utiliser une roue pour voir facilement quelle lettre correspond au message original (exemple : A=D, B=E).



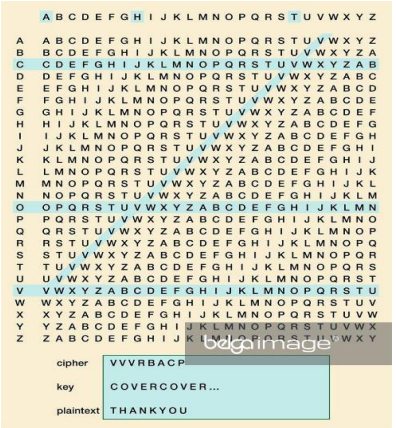
Wikicommons

9e siècle Analyse des fréquences

Le philosophe arabe Al-Kindi est le premier à décrire la cryptanalyse. Sa méthode utilise l'analyse des fréquences des lettres de l'alphabet. Certaines lettres sont plus courantes en fonction de langue écrite, on peut donc deviner ce qu'un caractère chiffré représente s'il est utilisé très souvent ou très rarement.

1457 Chiffrement par substitution polyalphabétique d'Alberti / de Vigenère

L'Italien Léon Battista Alberti utilise plusieurs alphabets pour chiffrer un message. L'avantage de ce système de substitution est qu'une lettre n'apparaît pas toujours de la même manière dans le texte chiffré. Un mot clé permet de savoir quelles versions de l'alphabet et dans quel ordre. Cette idée sera approfondie par le Français Blaise de Vigenère en 1586.



Wikicommons

1550 Grille de Cardan

Cette grille, inventée par Girolamo Cardano, consiste à cacher un message secret dans un texte apparemment sans importance. La grille est une feuille cartonnée dans laquelle sont découpés des rectangles disposés de façon variée au fil de la page. On écrit son message dans les rectangles et on remplit les vides par n'importe quel texte. Lorsqu'elle est posée sur le texte, la grille permet de faire apparaître le message secret qui y est caché.

1854 Babbage "casse" le chiffre de Vigenère

À l'origine de plusieurs découvertes scientifiques, Charles Babbage, inventeur britannique considéré comme un précurseur de l'informatique, dessine les plans de deux machines à calculer. Il est connu pour avoir cassé le chiffre de Vigenère.

1883 Principe du secret de la clé

Dans son traité *La Cryptographie militaire*, Auguste Kerckhoffs Van Nieuwenhof explique que la sécurité de la clé est plus importante que la sécurité de l'algorithme.

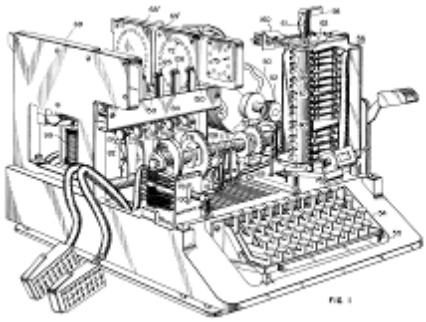
1918 Enigma

Cette machine cryptographique, mise au point par les Allemands Arthur Scherbius et Richard Ritter, utilise le chiffre de Vigenère. Composée d'un système de rotors (roues dentées qui tournent sur un axe) et de câbles changeant les combinaisons de lettres dans le message chiffré, la machine Enigma est d'un usage simple. Lorsque qu'une touche du clavier alphabétique est enfoncée, une lampe indique quelle est la lettre à substituer dans le cryptogramme. La clé étant changée chaque jour, le système paraissait incassable. Enigma a été utilisée par les Allemands durant la Seconde guerre mondiale.

© Belga

1941 Machine SIGABA

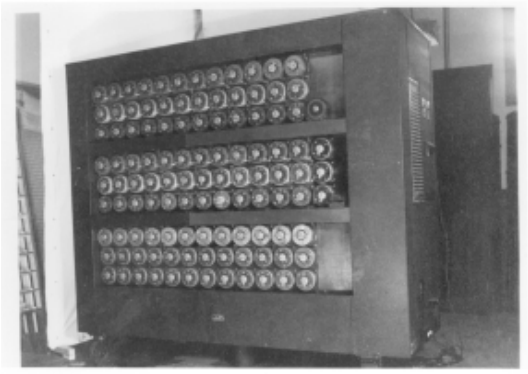
Machine de chiffrement utilisée par l'armée américaine pendant la Seconde Guerre mondiale et jusque dans les années 1950. Un mouvement aléatoire des rotors a rendu cette machine inviolable par les cryptanalystes.



Fichier : SIGABA-patent

1943 Alan Turing et les cryptanalystes britanniques cassent le code de la machine Enigma

Grâce à des travaux de mathématiciens et cryptanalystes polonais, les Britanniques (dont Alan Turing) parviennent à casser le code de la machine Enigma. Ils construisent leurs propres machines à calculer très puissantes, surnommées "bombes", qui testent toutes les combinaisons possibles. On estime que sans cette découverte, la guerre aurait duré deux ans de plus.



Coll. Bletchley Park

1976 Concept de clé publique et le principe d'échange de clé Diffie-Hellman

Whitfield Diffie et Martin Hellman imaginent la cryptographie à clé publique ou système de chiffrement asymétrique. Ce système utilise deux clés, une clé publique pour chiffrer (qui peut être diffusée) et une clé privée pour déchiffrer (qui doit rester secrète).

1977 DES (Data Encryption Standard)

Adoption du système de chiffrement symétrique (à une seule clé secrète) DES comme standard. Il repose sur le brouillage en 56 bits et en 16 tours. Émetteur et récepteur utilisent la même clé pour crypter et décrypter. Son fonctionnement est suffisamment complexe pour chiffrer les messages dans cette période où l'informatique se développe.

1977 RSA

Premier algorithme de chiffrement asymétrique décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman, le RSA utilise deux clés, l'une publique pour chiffrer et l'autre privée pour déchiffrer. Il est donc similaire au système imaginé par Diffie et Hellman. Cet algorithme protège très souvent l'échange de données sur Internet.

1991 PGP (Pretty Good Privacy)

Ce logiciel de cryptographie renforcée est créé par Philip Zimmermann, un informaticien américain. Il permet d'envoyer des messages chiffrés sur Internet, dont la lecture est impossible sans la clé de déchiffrement. Beaucoup de personnes aident encore actuellement Zimmermann à améliorer constamment ce logiciel gratuit et sûr et à le diffuser sur Internet.

1998 Libéralisation de l'usage de la cryptographie

La Belgique est une pionnière : profitant de la libéralisation des télécoms le 1er janvier 1998, le législateur a inséré dans la loi une disposition prévoyant que le cryptage est dorénavant libre.

2001 AES (Advanced Encryption Standard)

En 2000, l'algorithme Rijndael, élaboré par les Belges Joan Daemen et Vincent Rijmen (KULeuven) remporte le concours lancé par le National Institute of Standards and Technology (USA) afin de remplacer le DES. AES est devenu le standard international, reconnu entre autres par la NSA.

2008 Bitcoin

Crypto-monnaie électronique complètement virtuelle, elle s'échange sur des plateformes Internet. Cette monnaie, sans banque, est gérée par ses propres utilisateurs sur un réseau basé sur les principes de la cryptographie pour valider les transactions.

6. LES RESSOURCES EN BIBLIOTHÈQUE, MÉDIATHÈQUE ET SUR LE WEB

Ouvrages et site de référence

Simon Singh, *Histoire des codes secrets. De l'Égypte des pharaons à l'ordinateur quantique*, JC Lattès, 1999
http://www.editions-jclattes.fr/histoire-des-codes-secrets-9782709620482
→ LA référence, très bien écrit et accessible

Ars cryptographica, Une étude des messages secrets de l'Antiquité à nos jours par Didier Müller, Lycée cantonal de Porrentruy
https://www.apprendre-en-ligne.net/crypto/menu/index.html
→ Un site web très bien fait avec une foule d'explications et d'exercices en ligne

Sophie de Lastours, *Le chiffre, le renseignement et la guerre* - Actes du colloque de l'Historial de la Grande guerre de Péronne, L'Harmattan, 2001
http://www.eyrolles.com/Sciences/Livre/le-chiffre-le-renseignement-et-la-guerre-9782747524971

Pierre Berloquin, *Codes. La grande aventure*, Seuil, 2013 (coll. Points)
http://www.seuil.com/ouvrage/codes-pierre-berloquin/9782757825761

Pierre Berloquin, Codes. La grande aventure, Seuil, 2013 (coll. Points)
http://www.seuil.com/ouvrage/codes-pierre-berloquin/9782757825761

Bande dessinée

Hergé, *Les Aventures de Tintin - Le secret de la Licorne*, Casterman, 1943
https://fr.wikipedia.org/wiki/Le_Secret_de_La_Licorne

Edgar P. Jacobs et al., *Blake et Mortimer*, Le Lombard / Dargaud, 1950- (24 tomes)
https://fr.wikipedia.org/wiki/Blake_et_Mortimer

Alex Alice, Xavier Dorison, *Le Troisième Testament*, Glénat, 1997-2003 (4 tomes)
https://fr.wikipedia.org/wiki/Le_Troisi%C3%A8me_Testament#Publications_en_fran.C3.A7ais

Pour les plus jeunes

Philippe Nessmann, Emmanuel Cerisier, *Le monde des codes secrets*, Circonflexe, 2001
https://www.circonflexe.fr/catalogue/aux-couleurs-du-monde/le-monde-des-codes-secrets

Charles Dutertre, Michel Piquemal, Daniel Royo, *Le Grand Livre des codes secrets – Tout pour inventer de mystérieux messages*, Albin Michel, 2004
http://www.albin-michel.fr/ouvrages/le-grand-livre-des-codes-secrets-9782226150035

E. Zéda, D. Pic Lelièvre, *Les meilleurs codes secrets de tous les temps*, Casterman, 2006
http://www.ricochet-jeunes.org/livres/livre/29573-les-meilleurs-codes-secrets-de-tous-les-t

Les mathématiques

PETITS CONTES MATHÉMATIQUES - universciences.tv
http://www.universcience.tv/video-les-probabilites-5294.html?_ga=1.205206935.629139377.1474622441

COMMENT J'AI DÉTESTÉ LES MATHS, documentaire d'Olivier PEYON - 2013, France (en FR st. FM, AN. Durée : 99')
https://www.pointculture.be/mediatheque/documentaires/comment-j-ai-deteste-les-maths-tp1980/

Les révolutions populaires, les lanceurs d'alerte et les « hackers éthiques »

TAHRIR, PLACE DE LA LIBÉRATION, documentaire de Stefano SAVONA - 2011, Italie, France (en AR st. FR. Durée : 93')
https://www.pointculture.be/mediatheque/documentaires/tahrir-place-de-la-liberation-th8815/

WE STEAL SECRETS: THE STORY OF WIKILEAKS, documentaire de Alex GIBNEY - 2013, Etats-Unis (en AN, st. FR, NL, ES, IT, AN. Durée : 124')
https://www.pointculture.be/mediatheque/documentaires/we-steal-secrets-the-story-of-wikileaks-tq8800/

CITIZENFOUR, documentaire de Laura POITRAS - 2014, Allemagne / Etats-Unis / Royaume-Uni (en AN, st. FR. Durée : 114')
https://www.pointculture.be/mediatheque/documentaires/citizenfour-th1610/

The Internet's own boy, documentaire de Brian KNAPPENBERGER - 2014, Etats-Unis (en AN, st. FR. Durée : 105')
https://www.youtube.com/watch?v=7ZBe1VFy0gc

La Seconde guerre mondiale

ALAN TURING, LA RÉHABILITATION D'UN GRAND MATHÉMATICIEN - universciences.tv
http://www.cite-sciences.fr/fr/ressources/bibliotheque-en-ligne/portraits-de-savants/alan-turing/

GARBO L'ESPION - L'HOMME QUI SAUVA LE MONDE, documentaire d'Edmon ROCH - 2009, Espagne (en FR, AN, ES, AL, CA st. FR, ES, AN, CA, FM. Durée : 86')
https://www.pointculture.be/mediatheque/documentaires/garbo-l-espion-l-homme-qui-sauva-le-monde-th3611/

LA DRÔLE DE GUERRE D'ALAN TURING, documentaire de Denis VAN WAEREBEKE - 2014, France / Belgique (en FR. Durée : 60')
https://www.pointculture.be/mediatheque/documentaires/la-drole-de-guerre-d-alan-turing-tp2490/

Les codes au cinéma

LA GRANDE VADROUILLE, film de Gérard OURY - 1966, France (en FR. Durée : 135')
https://www.pointculture.be/mediatheque/cinema-fiction/la-grande-vadrouille-vg5901

UN HOMME D'EXCEPTION (A BEAUTIFUL MIND), film de Ron HOWARD - 2001, USA (en AN, FR st. AN, FR, NL, AR, BU. Durée : 136')
https://www.pointculture.be/mediatheque/cinema-fiction/un-homme-d-exception-vu8149

THE DA VINCI CODE, film de Ron HOWARD – 2006, USA (en AN, FR st. AN, FR, NL, AR, BU. Durée : 180')
https://www.pointculture.be/mediatheque/cinema-fiction/the-da-vinci-code-version-longue-vd0084

BENJAMIN GATES ET LE LIVRE DES SECRETS, film de Jon TURTELTAUB - 2007, Etats-Unis (en AN, FR. Durée : 124')
https://www.pointculture.be/mediatheque/cinema-fiction/benjamin-gates-et-le-livre-des-secrets-vb0689

SKYFALL, film de Sam MENDES - 2012, Royaume-Uni (en AN, FR. Durée : 142')
https://www.pointculture.be/mediatheque/cinema-fiction/skyfall-vs1602

ENQUÊTES CODÉES (THE BLETCHLEY CIRCLE), série de Andy DE EMMONY - 2012, Royaume-Uni (Langue AN, FR st. FR. Durée : 135')
https://www.pointculture.be/mediatheque/cinema-fiction/enquetes-codees-1-ve0626

THE IMITATION GAME, Morten TYLDUM - 2014, Royaume-Uni, USA (en AN, FR st. FR. Durée : 109')
https://www.pointculture.be/mediatheque/cinema-fiction/the-imitation-game-vi0388

7. LES ANIMATIONS PROPOSÉES

Découvrez le monde des codes secrets, du chiffrement et du décryptage grâce à un parcours guidé de l'exposition, ou grâce à diverses animations spécifiques proposées par le Mundaneum et ses partenaires.

- **VISITE GUIDÉE** (FR – NL – EN)

Dès 8 ans – Durée : 1h30 – PAYANT **(75,00€ + entrée à l'exposition)**

Un parcours guidé dans l'exposition : histoire des codes et des machines, focus sur la Seconde guerre mondiale, sécurité informatique, ... Adaptation possible aux besoins du groupe.

- **ATELIER ON NOUS PRENDS POUR DES C***!?! (ACTION MÉDIAS JEUNES)**

Dès 15 ans – Durée : 1h – PAYANT – **de février à mai 2018**

Composé d'une découverte guidée de l'univers «Top secret! Un monde à décrypter» suivie d'un atelier : "**Construis ta propre théorie du complot**". L'atelier consiste en une création de fausse théories complotistes qui prendront la forme d'articles web. Grâce à cette animation, les jeunes seront plus critiques dans leur rapport à l'information en apprenant à repérer les logiques de la désinformation et en s'appropriant les codes des théories du complot.
Dates payantes disponibles sur demande. Chaque atelier se donnera par groupe de 15.
Uniquement sur inscription: info@mundaneum.be ou 065/31.53.43

- **ATELIER PHILO: LE SECRET SOUS TOUTES SES FORMES**

Dès 6 ans – Durée : 1h30 – GRATUIT **(+ entrée à l'exposition payante)**

L'animation philosophique permet une discussion respectueuse de chacun, développe le sens de la logique et exerce la pensée. L'animateur est un guide, un arbitre mais pas un maître à penser : c'est le groupe lui-même qui imagine la question au cœur du débat !

- **ATELIER: INITIATION AU CODE INFORMATIQUE**

Dès 8 ans – Durée : 1h30 – GRATUIT **(+ entrée à l'exposition payante)**

N'importe qui peut apprendre les bases du code informatique, surtout en s'amusant ! Pour que les plus jeunes ne soient pas de simples consommateurs mais des acteurs de la société numérique, une initiation au code informatique est le premier pas. Dates sur demande.

- **ANIMATION: MUNDAVENTURE**

Dès 8 ans – Durée : 1h30 – PAYANT -! **à partir d'avril 2018**

Jeu de société : Stopper l'expansion du trou noir en sauvegardant les connaissances. Pour cela, vous devrez réussir à sauvegarder plus de centres de connaissance que le trou noir et ainsi, garantir la pérennité de l'humanité.

- **ANIMATHIONS TOP SECRÈTES**

Dès 10 ans – Durée : 1h30 – PAYANT – **! seulement disponible les lundis et mardis**

1 aniMATHion : 125,00 € - 2 aniMATHions / jour : 215,00 € - 3 aniMATHions / jour : 300,00 €

- **P5-P6:** Mets-toi dans la peau de François Viète, mathématicien de génie et grand déchiffreur du roi de France. Après avoir découvert le célèbre code " cassette ", sur base d'additions et de soustractions simples associées à l'alphabet, déchiffre les messages laissés par François et réponds-lui en chiffrant tes propres courriers.

- **S1-S2:** De l'époque romaine à la nôtre, la cryptographie a toujours été présente. Revis son évolution historique à travers des codes de plus en plus complexes à déchiffrer. Tu réaliseras des enchaînements d'opérations mais attention, parfois, des nombres entiers négatifs apparaitront. Le signe du résultat changera complètement le décodage du message...

- **S3-S4:** Un mathématicien belge, connu sous le pseudonyme de " Minos ", a créé pour toi des cryptarithmes. Il s'agit de casse-têtes numériques qui consistent en une équation mathématique. Sa résolution passe par la déduction et l'utilisation d'astuces de calculs.

- **S5-S6:** Sans le savoir, tu as probablement déjà utilisé le " code de César ", un code que César utilisait pour communiquer secrètement avec ses généraux. Mais connais-tu le code d'Alberti et surtout celui de Vigenère utilisé encore il y a moins de 100 ans ? Découvre pourquoi les nombres premiers sont la clé de voûte du système bancaire actuel et enfin, démasque comment les codes secrets vont te permettre de réaliser un tour de magie... épatant !

8. LES ÉVÈNEMENTS POUR LES ENSEIGNANTS ET OPÉRATEURS ASSOCIATIFS

LE 11 OCTOBRE 2017 DÈS 13H00

Vernissage enseignants, associations et familles

Au programme :

- Découverte libre de l'exposition
- Spectacle participatif NoodleBrain par Arts Nomades

LE 14 NOVEMBRE 2017 À 18H00

Table-ronde CoGame

Jeu vidéo amateur, patrimoine, culture et citoyenneté.
Avec Pierre-Yves Hurel (Arts&Publics, ULg), Julien Annart (Gaming out, Quai 10).
Un projet Erasmus+

DISCLAIMER
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

LE 8 FÉVRIER 2018 À 10H00

"ON NOUS PREND POUR DES C***!?!"

Pour les jeunes et adultes dès 16 ans

Journée d'ateliers et de débat sur les théories du complot et les "fake news".
Avec la Maison de la Presse Mons.

BONUS

DU 3 AU 6 AVRIL

Stage de Pâques 2018 (avec le Plaza Art)

Pour les enfants de 7 à 11 ans

Deviens un super agent secret et réalise ton film !
Du mardi 3 au vendredi 6 avril 2018 - De 9h à 16h - Prix : 70€/semaine

INFORMATIONS PRATIQUES

Exposition : FR - NL - EN
Visites guidées : FR - NL - EN - DE

MUNDANEUM

Rue de Nimy, 76
7000 Mons
www.mundaneum.org
info@mundaneum.be - +32 (0)65 31 53 43

Horaires d'ouverture :

MER-VEN	13h-17h
SAM-DIM et jours fériés	11h-18h

Fermé le lundi et le mardi, le 25 décembre et le 1er janvier
Possibilité de visite guidée du lundi au dimanche de 9h à 16h **(sur réservation uniquement)**

Tarifs

Visites libres

Adultes (26-64)	7,00€
Seniors (+65), groupes adultes	5,00€
Demandeurs d'emploi / RIS, enfants et étudiants (-26)	2,00€
Article 27	1,25€ + 1 ticket A27
Accompagnateurs Article 27	Gratuit
Carte Prof / Lerarenkaart	Gratuit
Premier dimanche du mois (tout public)	Gratuit
Carte Culture UCL	1 entrée GRATUITE pour 1 entrée PAYANTE au tarif étudiant

Visites guidées et animations

Sur réservation

Durée : 1h30

Max. 25 pers. par guide / animateur

Tarif (sauf animations partenaires) :

75,00 € par guide / animateur
+ 2,00 € par personne (adultes et seniors)
+ 1,25 € par personne (scolaire, étudiants, demandeurs d'emploi, Article 27)

Tickets combinés

- Collectionneurs d'idées – Avec la Maison Losseau (Rue de Nimy, 37-39 - 7000 Mons)
- Unesco Go – Avec le Bois-du-Luc / Musée de la Mine et du Développement Durable (Rue Saint Patrice 2b - 7110 Houdeng-Aimeries)

mundaneum

Top secret!

#TOPSECRETXPO

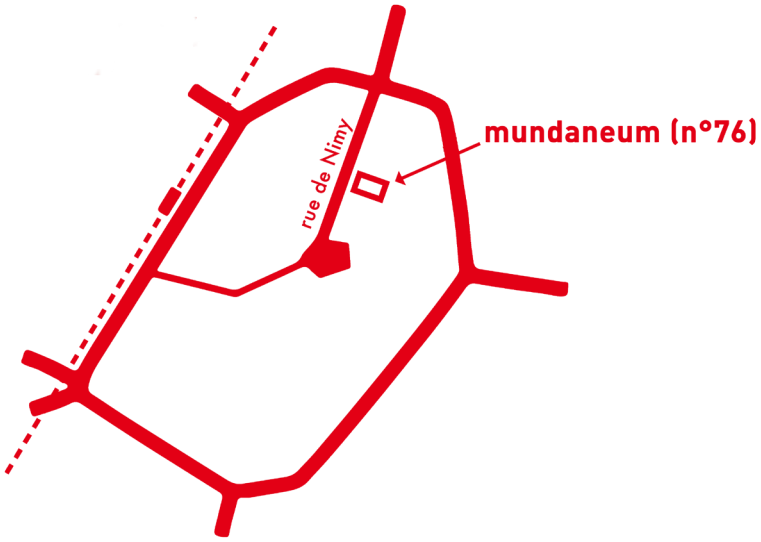
UCL Université catholique de Louvain

10.10.2017 - 20.05.2018

Une exposition organisée par le Mundaneum avec l'Université catholique de Louvain et UCL Culture
Avec le soutien de la Fédération Wallonie-Bruxelles, la Wallonie et la Province de Hainaut

Mundaneum
Rue de Nimy 76
7000 Mons
BELGIUM
www.mundaneum.org
info@mundaneum.be
+32 (0)65 31 53 43

Contact pédagogique
Nicolas Brunel
Assistant archiviste et service éducatif
nicolas.brunel@mundaneum.be
Tel: +32 (0)65 39.54.84



B
15 min.

TEC
3 min.

P €
Place du Parc

P €
Boulevard J.F. Kennedy

#TOPSECRETXPO