

N<sup>o</sup> AZDB-

ÉDITION FRANÇAISE



UCL  
Université  
catholique  
de Louvain

# UN MONDE À DÉCRYPTER

## ÉDITO

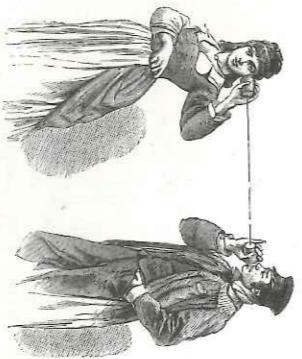
p. 00002

EXPOSITION



QUELQUES  
REPÈRES  
CHRONOLOGIQUES

p. 00012



TOP SECRET!

10.10.2017 - 20.05.2018

@ MUNDAEUM,  
MONS



p. 00016

p. 00014

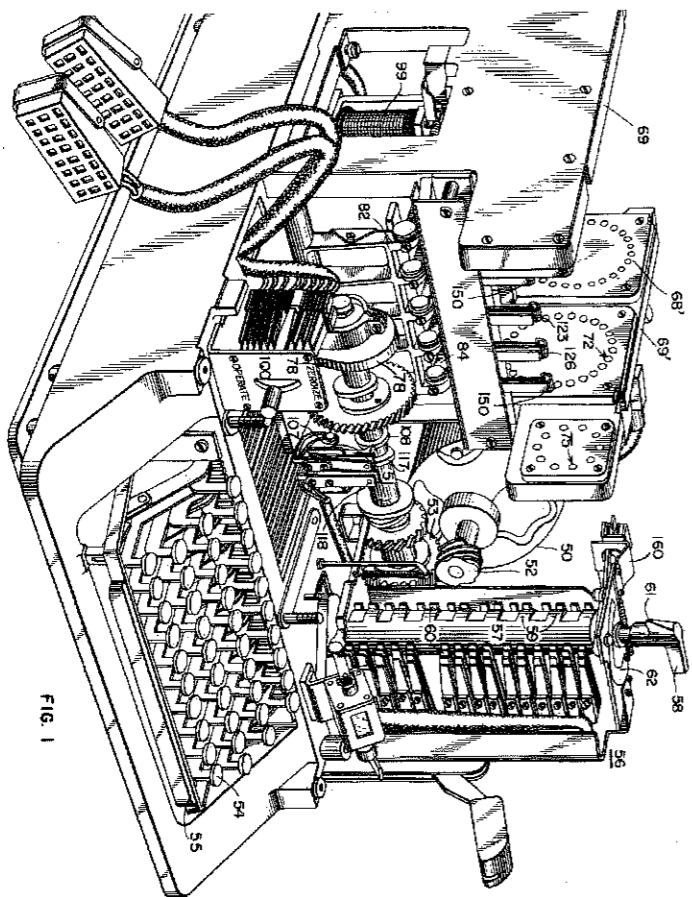


FIG. 1

## UN MONDE À DÉCRYPTER

La cryptographie, ou l'art de l'écriture secrète, est un enjeu important de la société actuelle. Le développement du numérique, l'usage intensif des communications et les innombrables applications en ligne ont engendré un besoin accru de sécurisation de l'information et des technologies qui y sont liées.

L'apparition de la cryptographie coïncide avec celle des premières écritures. Très tôt, l'écriture suscite le besoin de moyens de communication sûrs, en particulier

chez

auprès des gouvernements et des armées. Les usages de la cryptographie n'ont dès lors cessé de

se multiplier, jusqu'à envahir notre quotidien. Son histoire, étroitement liée à l'évolution des sciences et des techniques, est déterminée par la nécessité permanente pour les concepteurs de systèmes de cryptographie, les cryptologues, de contrer les attaques des cryptanalystes (les «déserteurs» ou les «hackers» d'aujourd'hui). Cette lutte a poussé les uns et les autres à élaborer

des techniques et des méthodes

# EDIT Top Secret!

▲ Chiffrement d'une dépêche à Paris, [1920-1939]

Machine SIGABA.  
Machine de chiffrement utilisée par l'armée américaine pendant la Seconde Guerre mondiale et jusqu' dans les années 1950.



# UN MONDE DE CODES ET DE VÉROUS

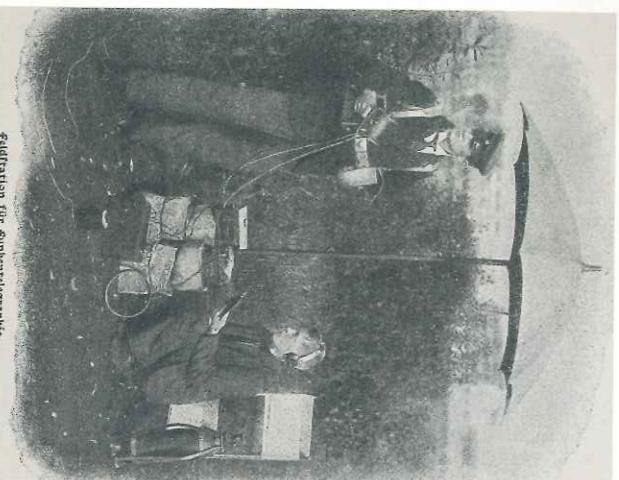
Imaginez une société sans secret: un espace-temps où tout le monde pourrait tout savoir... Difficile à concevoir! Que ce soit sous la forme de clés, de coffres forts, de cadenas ou encore de leurs pendants numériques, la sécurité est partout. Il suffit d'observer nos objets du quotidien pour réaliser à quel point l'homme tient à protéger ce qui lui est cher ou vital. Cette préoccupation s'étend aux informations qu'il concerne, qu'il utilise et qu'il échange. À l'heure du «tout connecté» et de la numérisation des services, le citoyen est confronté à d'importantes questions en termes de sécurité informatique, de protection de sa vie privée, de son identité et de cybersécurité. La progrès promis par la technologie doit toujours composer avec les multiples risques potentiels, et nous aspirons tous à la confiance numérique. ■



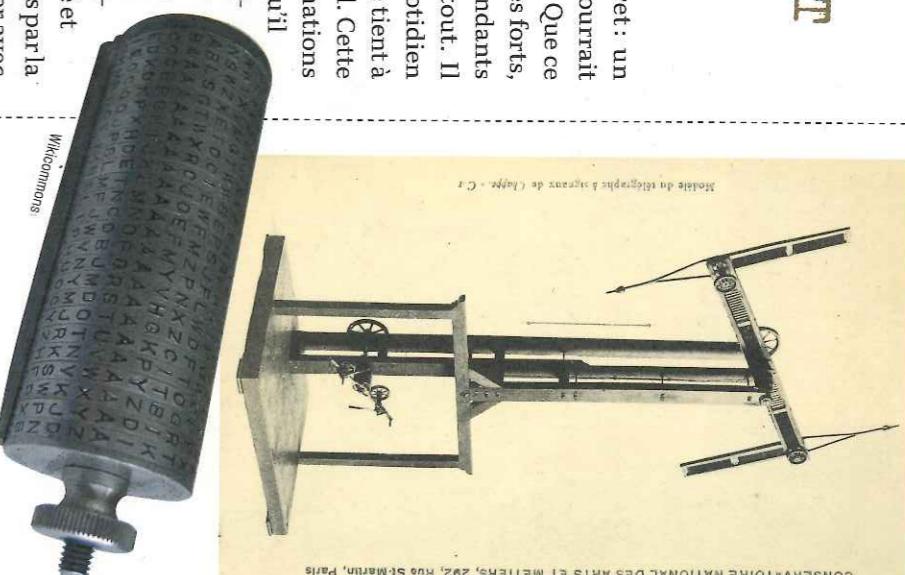
## LE CHIFFRE DE MARIE

Accusée d'avoir assassiné son second mari, la reine d'Écosse, Marie Stuart (1542-1587) est emprisonnée en 1568 par sa cousine, la reine d'Angleterre Elizabeth I<sup>e</sup> (1533-1603). La vraie motivation de cet emprisonnement est d'écartier Marie du trône. Catholique, celle-ci était soutenue par les catholiques anglais, au contraire d'Elizabeth qui était de confession anglicane et dont ils contestaient la légitimité. Elizabeth est en effet le fruit du mariage entre Henry VIII et Anne Boleyn, conclu après son divorce non reconnu par le pape de Catalogne d'Aragon. En prison, Marie échange des lettres relatives à un projet d'assassinat d'Elizabeth. Sa correspondance est cryptée mais décryptée par les services d'espionnage d'Elizabeth grâce à l'analyse des fréquences. Jugée coupable de complot, Marie Stuart est décapitée en 1587.

Station de télégraphie sans fil

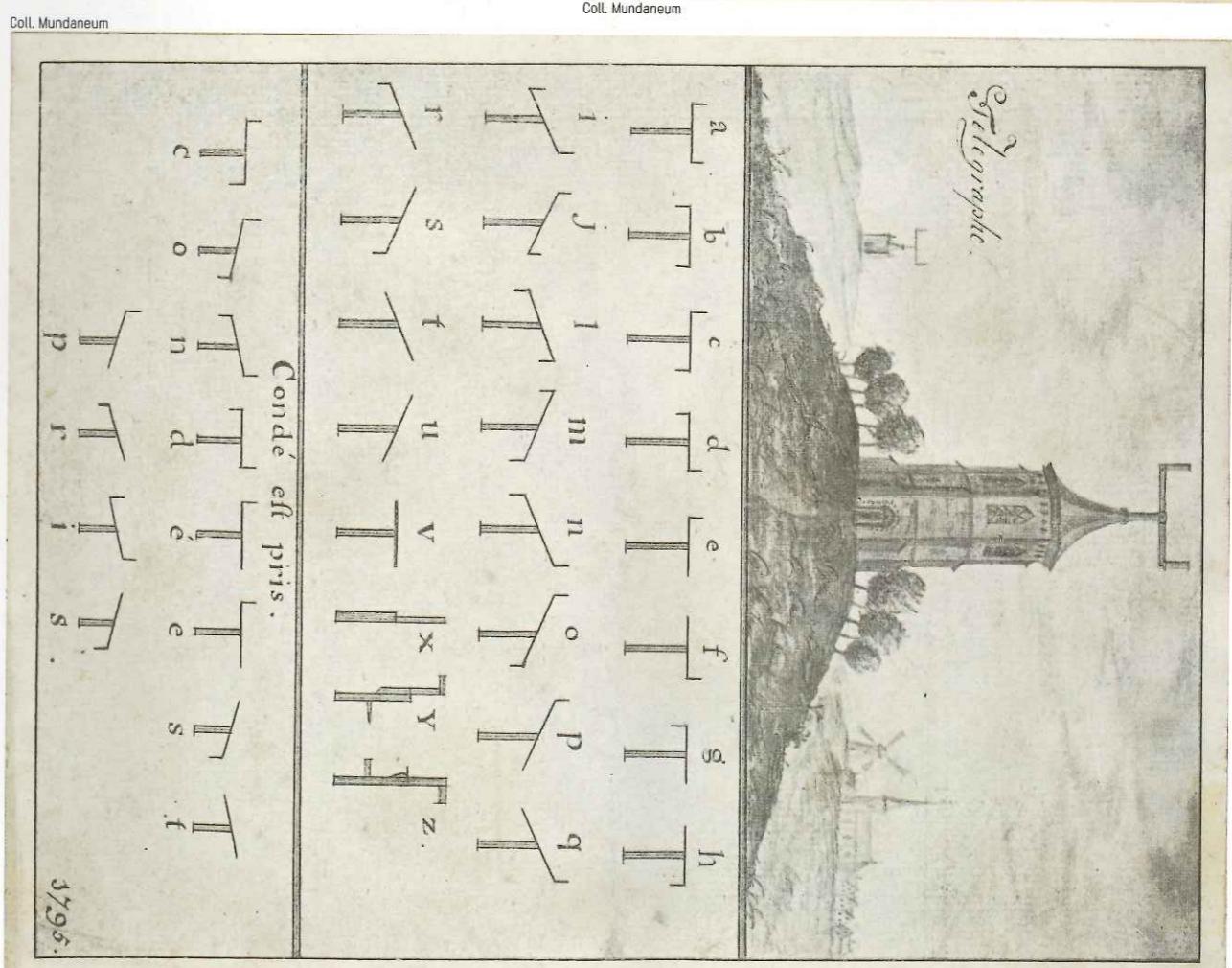


Coll. Mundaneum



Cylindre de Jefferson. Du nom de Thomas Jefferson, 3<sup>e</sup> président des États-Unis (1801-1809), il permet de chiffrer et de déchiffrer un message.

Télégraphe Chappe (1794). Ce télégraphe optique repose sur un mécanisme placé sur un point proéminent, visible de loin, permettant de communiquer grâce à un code visuel.



Cryptographie	
a	b
c	d
i	j
n	m
o	p
q	r
s	t
u	v
x	y
z	

personne qui les réceptionne, renforce l'usage de la cryptographie.

Lors de la Première Guerre mondiale, une véritable course au chiffrement et au déchiffrement se livre entre les armées. La plupart des codes et algorithmes existants sont cassés. C'est à cette période que les premières machines à chiffrer voient le jour. La plus connue est l'Enigma (1918), qui sera utilisée par les Allemands jusqu'à la Seconde Guerre mondiale.

Pendant longtemps, la cryptographie est en retard sur la cryptanalyse. Cela évolue avec l'arrivée des machines mécaniques et électromécaniques.

Jusqu'au 19<sup>e</sup> siècle, les méthodes de chiffrement sont relativement faibles, parce que la cryptographie est manuelle jusqu'en 1914 et parce que jusqu'à la fin du 18<sup>e</sup> siècle, les messages sont transmis par des moyens non mécanisés: le coursier, la fumée, la lumière ou encore le bruit (les 3 derniers éléments étant difficilement maîtrisables).

Les premiers codes élaborés apparaissent avec le télégraphe de Chappe (1794). L'appareil permet de maîtriser la transmission du signal mais pour éviter que le message ne puisse être compris par d'autres personnes que le destinataire, il nécessite l'utilisation d'un code. La télégraphie (1837), qui permet de transmettre des messages sur de longues distances mais sans certitude sur l'identité de la

vraiment. ■

## LA CRYPTOGRAPHIE AU FIL DU TEMPS

L'histoire de la cryptographie débute 3000 ans avant notre ère, lorsqu'apparaît l'écriture et, avec elle, la nécessité de protéger les messages échangés. Elle retrace la «bataille acharnée» que se livrent les cryptothéoriciens, qui créent les algorithmes de chiffrement des messages, et les cryptanalystes, qui tentent de les déchiffrer.

Les systèmes cryptographiques ont évolué avec les connaissances et les techniques, notamment en matière de communication. De l'Antiquité à nos jours, quatre périodes se démarquent: la cryptographie manuelle, la cryptographie mécanique (et électromécanique), la cryptographie moderne ou numérique, et la cryptographie quantique.

Jusqu'au 19<sup>e</sup> siècle, les méthodes de chiffrement sont relativement faibles, parce que la cryptographie est manuelle jusqu'en 1914 et parce que jusqu'à la fin du 18<sup>e</sup> siècle, les messages sont transmis par des moyens non mécanisés: le coursier, la fumée, la lumière ou encore le bruit (les 3 derniers éléments étant difficilement maîtrisables).

Les premiers codes élaborés apparaissent avec le télégraphe de Chappe (1794). L'appareil permet de maîtriser la transmission du signal mais pour éviter que le message ne puisse être compris par d'autres personnes que le destinataire, il nécessite l'utilisation d'un code. La télégraphie (1837), qui permet de transmettre des messages sur de longues distances mais sans certitude sur l'identité de la

vraiment. ■

# LA CRYPTANALYSE POUR GAGNER LA GUERRE

La Seconde Guerre mondiale marque les débuts de l'ère de la guerre de l'information. Le secret y occupe une place fondamentale, il fait partie du quotidien des armées et de la Résistance. Décrypter les messages de l'ennemi constitue un enjeu majeur.

Les Allemands bénéficient en effet d'un avantage considérable : l'Enigma. Ce cryptographe, qui fêtera son centenaire en 2018, est une des premières machines de cryptographie. Popularisée par le film *The Imitation Game* (2014), son fonctionnement était d'une complexité inédite. Les Polonais étaient parvenus à en décoder les messages peu avant la guerre mais les

Allemands en avaient renforcé la sécurité et elle était réputée incassable.

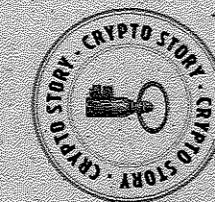
Lorsque la guerre éclate, personne n'était encore parvenu à trouver la solution pour déchiffrer les messages qui en sortaient.

Après des mois de travail, une équipe rassemblée par les services secrets britanniques à Bletchley Park, un domaine situé au Nord de Londres, y parvient pourtant. Composée de cryptologues, de mathématiciens, de linguistes parmi lesquels compte le pionnier de l'informatique Alan Turing, elle vaincra l'Enigma et jouera un rôle déterminant dans la victoire des Alliés. ■



© Belga

**MURAILLE DE CHINE**  
Les camps militaires de la muraille de Chine communiquaient par messages cryptés pour prévenir les invasions, au moyen de feux ou de roulements de tambours relayés de tour en tour.



## CRYPTO STORY

Les camps militaires de la muraille de Chine communiquaient par messages cryptés pour prévenir les invasions, au moyen de feux ou de roulements de tambours relayés de tour en tour.

Service Beagle, [1942-1944].

Beagle est un service de renseignements météorologiques de la Résistance belge.

Le contenu de ses messages a permis de déchiffrer des messages allemands, grâce à la comparaison des prévisions météorologiques qu'ils contenaient.



Coll. Cégesoma

# BLETCHLEY PARK, LE DOMAINE DES CASSEURS DE CODES \*

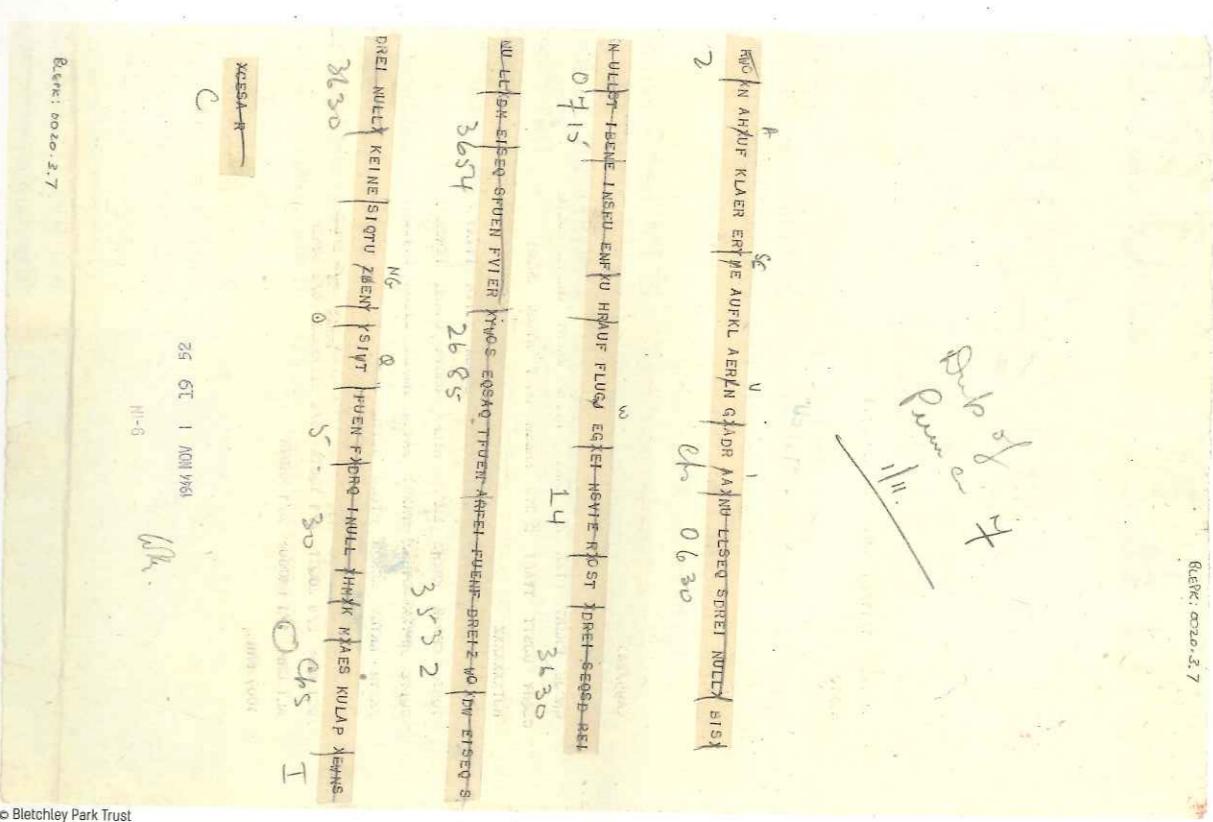
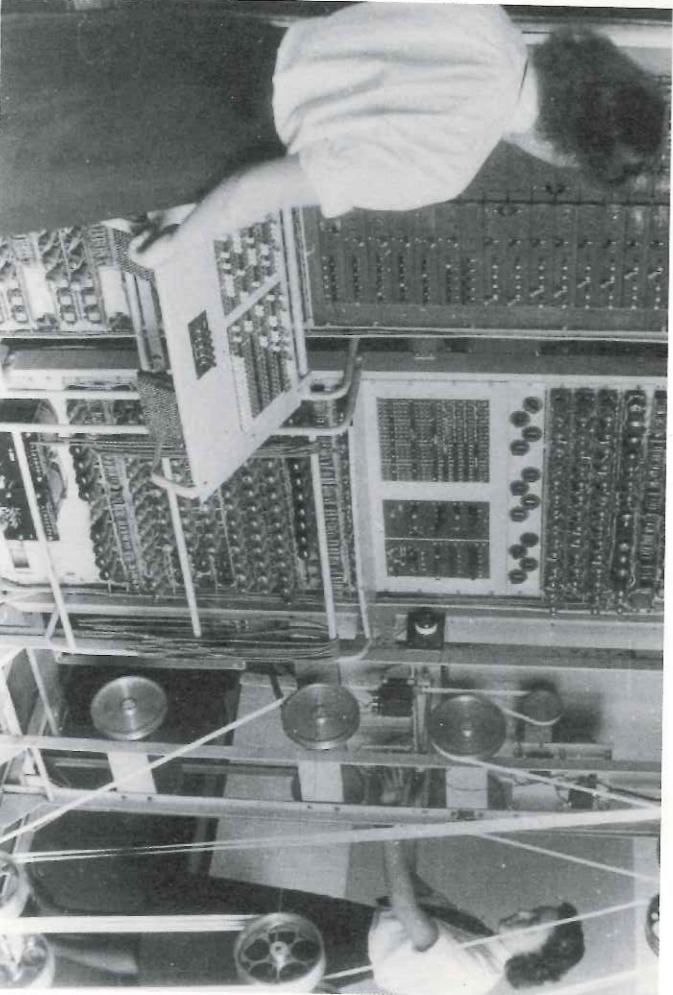
À l'origine station secrète de réception et démission radio, Bletchley Park est situé à 60 km au nord de Londres. En 1938, le MI6 (le service des renseignements du Royaume-Uni) y installe la *Government Code and Cypher School* qui deviendra le principal centre de décryptage du pays pendant la Seconde Guerre mondiale. Le travail mené à Bletchley Park par cette équipe de mathématiciens, de linguistes et de cryptologues, contribuera à écarter la Seconde Guerre mondiale. Son objectif: casser le code des machines Enigma et Lorenz que les Allemands utilisent pour chiffrer leurs messages, ce qu'ils réussissent à faire en 1943.

Bletchley Park est alors une véritable usine du renseignement: jusqu'à 1000 personnes y sont actives jour et nuit pour faire

gagner aux Alliés la guerre de l'information. Toutes les activités sont top secrètes, et les collaborateurs tenus à la réserve la plus absolue sur leur implication dans le projet. Leur travail a joué un rôle notamment dans la réussite du débarquement du 6 juin 1944, dans le déchiffrement des codes japonais ou encore dans l'aboutissement de la Guerre du Pacifique (entre les Alliés et le Japon).

À la fin de la guerre, une grande partie de l'équipement est détruit et les collaborateurs s'engagent à garder le secret. Celui-ci ne sera levé que dans les années 1970. ■

\* Textes inspirés des expositions virtuelles publiées par Bletchley park sur la plateforme Google arts et culture.



Machine Colossus manipulée par des membres du Women's Royal Naval Service

Les casseurs de code au travail à la hutte 6



## LES AGONY COLUMNS

Dans l'Angleterre victorienne du 19<sup>e</sup> siècle, les jeunes gens amoureux n'étaient pas autorisés à manifester leurs sentiments. Sachant que leurs lettres seraient interceptées et lues par leurs parents, ils s'envoyaient des messages cryptés dans les rubriques d'annonces personnelles des journaux (baptisées en Angleterre les *agony columns*). Cela suscita la curiosité des cryptanalystes qui s'amusaient à déchiffrer leur excitant contenu. Dès lors, les cryptographes insérèrent des messages cryptés dans les journaux pour provoquer leurs collègues ou encore pour critiquer des personnalités ou des institutions.

# ALAN TURING

(1912-1954)

*Qu'il soit poète,  
artiste, musicien,  
physicien ou  
mathématicien,*

*le génie ne se résume*

*pas. Il est lui-même*

*un résumé,*

*un raccourci,*

*une voie que*

*personne n'avait osé*

*emprunter avant lui.*

*Alan Turing*

réunis sur le site topsecret. L'approche originale de Turing se base, dans une optique de rétro-ingénierie, sur l'exploitation des imprudences des chiffreurs allemands. Son travail transformera la cryptanalyse en une branche des mathématiques. Bien que les opérations menées à Bletchley Park aient contribué à mettre fin à la guerre, celles-ci resteront secrètes jusque dans les années 1970.

pardon aux hommes incriminés à l'époque où l'homosexualité était encore considérée comme illégale au Royaume-Uni.

## LE MATHÉMATICIEN, PRÉCURSEUR DE L'INTELLIGENCE ARTIFICIELLE

Fils d'un fonctionnaire de l'administration coloniale en Inde, Alan Turing naît à Londres en 1912 et est élevé par des amis de la famille. Très jeune, il montre un goût prononcé pour les chiffres et les énigmes.

À l'adolescence, il rencontre Christopher Morcom, inscrit comme lui à la Sherborne School et dont il partage le goût pour les mathématiques et les sciences. Il noue avec lui une amitié profonde qui influence le cours de sa vie. La mort prématurée de Morcom ébranle Turing. Plus tard, il étudie les mathématiques au King's College de Cambridge où il assume ses préférences sexuelles malgré le climat de réprobation de l'époque. Il sera « Visiting Fellow » à l'Université de Princeton (USA), et travaillera après la guerre au National Physical Laboratory à Londres puis à l'Université de Manchester. Élu « Fellow » de la Royal Society, il développe une théorie de morphogenèse ou théorie mathématique de biologie organique.

Ses brillantes contributions à la science et à l'effort de guerre ne le protègent pas de la persécution de l'Etat britannique. Inculpé d'« indécence manifeste et de perversion sexuelle », Alan Turing doit choisir entre l'incarcération ou la castration chimique. Le traitement a de lourds effets secondaires sur les plans physique et moral. Alan Turing est retrouvé mort par empoisonnement le 8 juin 1954 à sa maison à Wilmslow, Cheshire. ■



Coll. King's College Library, Cambridge

Mathématicien et cryptologue britannique, Alan Mathison Turing est aujourd'hui considéré comme le père de l'informatique moderne. Décédé préma- turément à l'âge de 41 ans, Alan Turing a exprimé son génie dans les mathéma- tiques, la cryptologie, la biologie et l'infor- matique. Doué depuis sa plus tendre en- fance pour résoudre énigmes et problèmes complexes, il est parvenu à casser les codes secrets de l'armée allemande durant la Seconde Guerre mondiale. Homosexuel, sanctionné par la justice britannique pour faits d'« indecience grossière », son nom est aujourd'hui associé à un amendement nommé « Loi Alan Turing » qui accorde le

pardon aux hommes incriminés à l'époque où l'homosexualité était encore considérée comme illégale au Royaume-Uni. Whifffield Diffie et Martin Hellman (USA) considérés comme les inventeurs des tech- niques de chiffrement moderne.

## L'HOMME

En 1938, Alan Turing collabore avec le gouvernement britannique sur des opérations de déchiffrement de codes de l'armée allemande. Il fait partie des jeunes cervaeux appelés à rejoindre le site de Bletchley Park au Nord de Londres, où il travaillera pour les services secrets britanniques (MI6) et la Government Code and Cypher School. Son travail consiste à décrypter les messages chiffrés par la machine Enigma. Là, il contribue à la mise au point d'une « bombe », une machine électromécanique capable d'abattre le travail de déchiffrage quotidien des milliers de collaborateurs

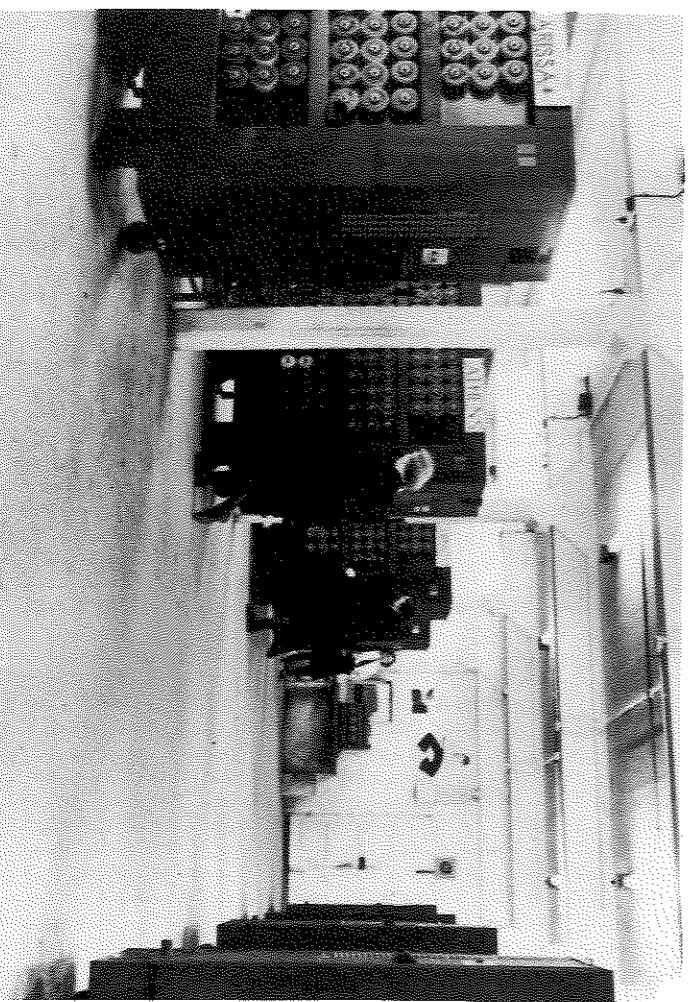
d'opérations de routine. Il pose le postulat suivant : si par le « jeu de l'imitation », un ordinateur arrive à faire croire à un humain qu'il interagit avec un autre humain et non avec une machine, il convient alors de parler d'intelligence artificielle. Cette idée simple s'avèrera par la suite extrême- ment influente, et le test de Turing restera longtemps sans équivalent.

## LE CASSEUR DE CODES

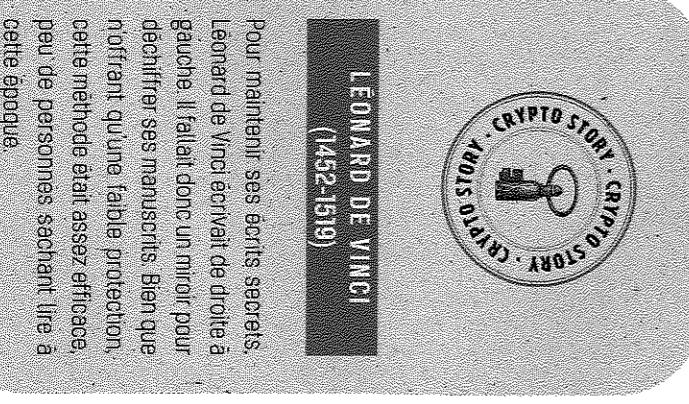
En 1938, Alan Turing collabore avec le gouvernement britannique sur des opérations de déchiffrement de codes de l'armée allemande. Il fait partie des jeunes cervaeux appelés à rejoindre le site de Bletchley Park au Nord de Londres, où il travaillera pour les services secrets britanniques (MI6) et la Government Code and Cypher School. Son travail consiste à décrypter les messages chiffrés par la machine Enigma. Là, il contribue à la mise au point d'une « bombe », une machine électromécanique capable d'abattre le travail de déchiffrage quotidien des milliers de collaborateurs

*Les tentatives de création de machines pensantes nous seront d'une grande aide pour découvrir comment nous pensons nous-mêmes.*

Alan Turing



Coll. Bletchley Park Trust



LÉONARD DE VINCI  
(1452-1519)

Pour maintenir ses écrits secrets, Léonard de Vinci écrivait de droite à gauche. Il fallait donc un miroir pour déchiffrer ses manuscrits. Bien que n'offrant qu'une faible protection, cette méthode était assez efficace, peu de personnes sachant lire à cette époque.

Eastcote Greek  
Bombay Bay

# DES MACHINES INTELLECTUELLES À L'INTELLIGENCE ARTIFICIELLE

Tout semble à première vue opposer le Britannique Alan Turing (1912-1954) et le Belge Paul Otlet (1868-1944), fondateur du Mundaneum. Le premier est mathématicien, le second est juriste et bibliographe. Turing pose les bases de l'informatique et de l'intelligence artificielle, Otlet est reconnu comme le père de la documentation. Pourtant, bien que peu reconnus à leur décès, tous deux sont pionniers et visionnaires des technologies et des sciences de l'information.

«Classer est la plus haute opération de l'esprit, celle qui implique toutes les autres. L'esprit s'élève à mesure qu'il est susceptible d'abstraction, de systématisation et de synthèse» écrit Paul Otlet dans son *Traité de documentation* (1934). Initiés dans les années 1890, ses travaux se recentrent au début du 20<sup>e</sup> siècle sur une alternative à trouver au livre traditionnel, dont il trouve le format figé inadapté à la croissance exponentielle de l'information. Dans son *Traité*, Paul Otlet évoque les «machines intellectuelles». À la croisée de l'humain

prolongements à la fois des organes de la perception, des organes de la mémoire et du raisonnement, et des organes de l'action et de l'expression. Paul Otlet entrevoit l'utilité de ces « machines intellectuelles » pour le travail scientifique notamment. ■

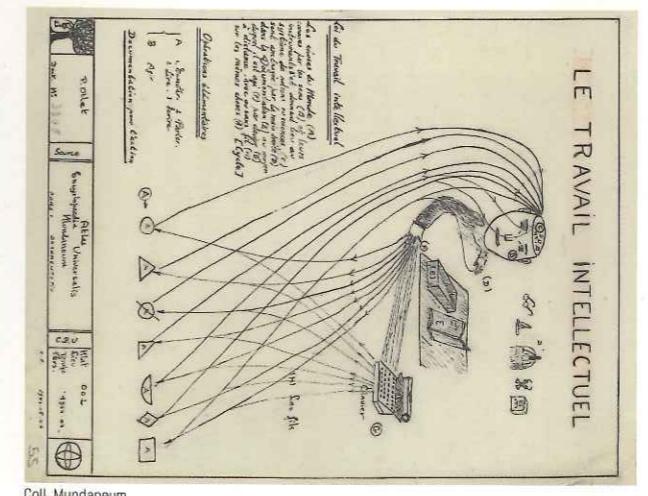
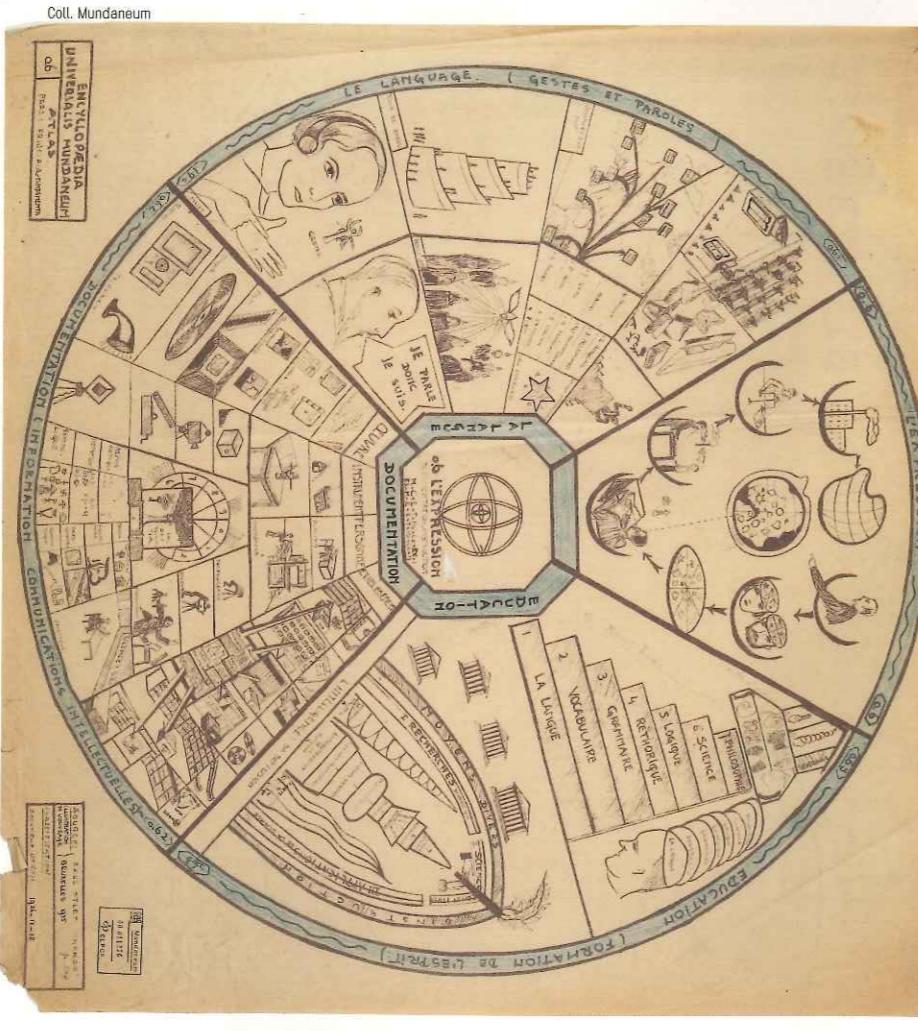
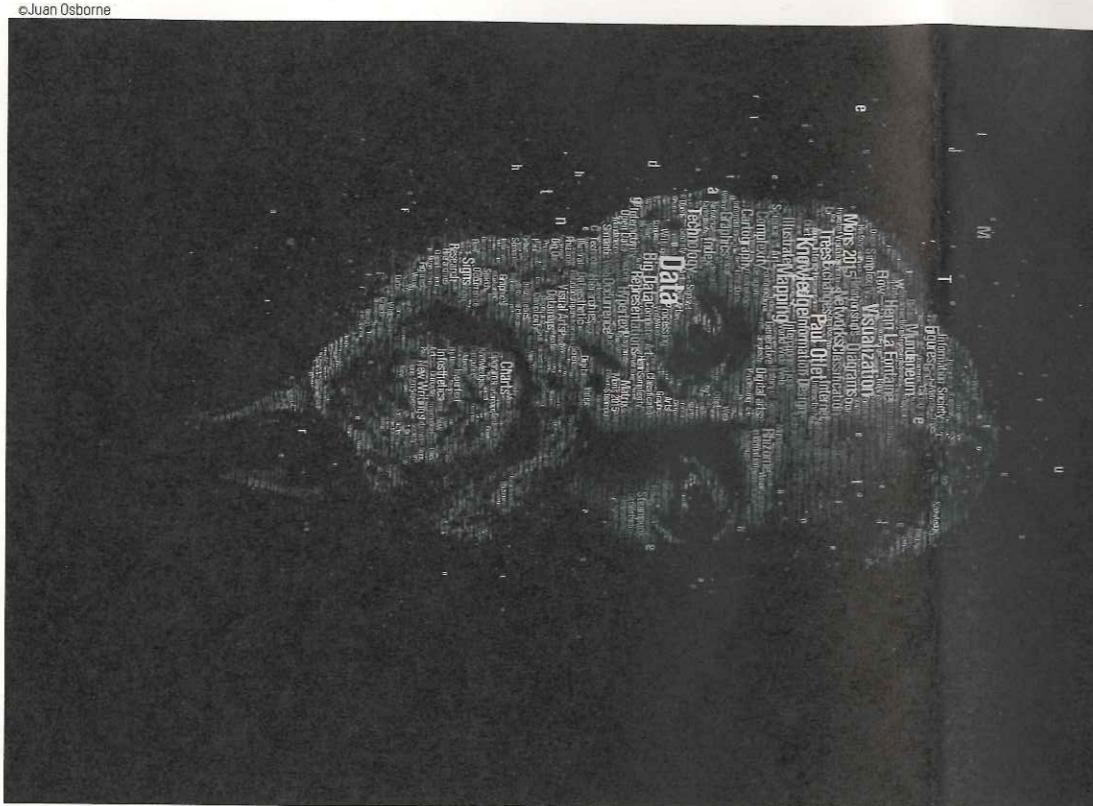


Schéma (1944) et panneau (1935) de l'*Encyclopaedia Universalis Mundaneum*,



Alan Turing et Paul Otlet, par Juan Osborne.  
Architecte, designer et programmeur, Juan Osborne (Madrid) a créé ses propres techniques et outils afin de créer ses illustrations en images de mots.



# BALADE DANS LES PROFONDEURS DU WEB...



## LE CHAPEAU FAIT LE HACKER!

To **hack** en anglais signifie « découper » quelque chose, c'est-à-dire: décomposer pour recomposer, « bidouiller », bricoler!

Le symbole du chapeau évoque l'univers de la piraterie.

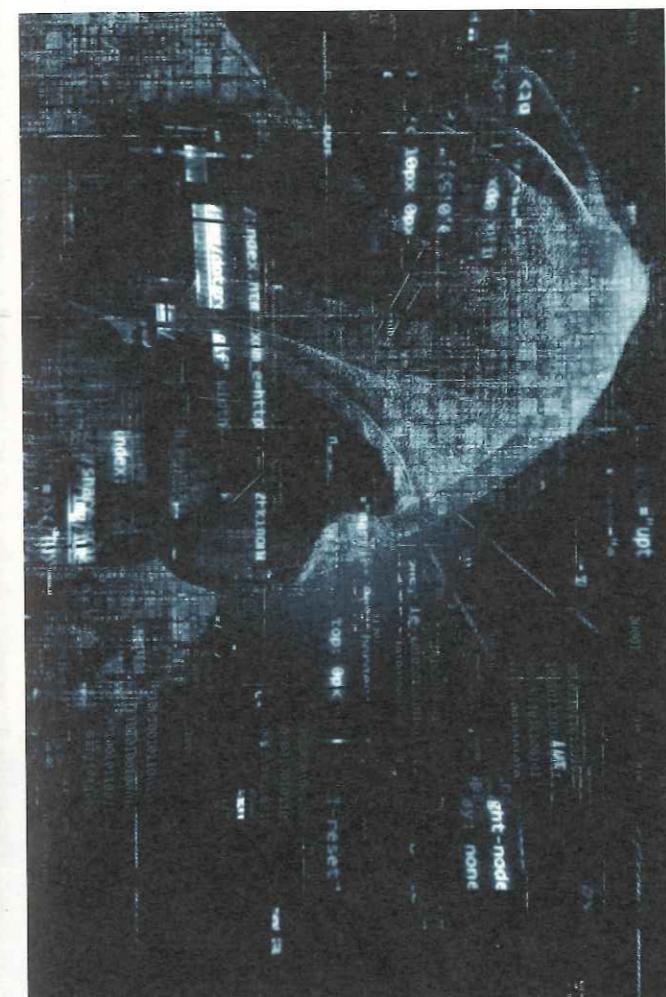
**Black Hat**: Pirate informatique qui pénètre les systèmes informatiques avec l'intention de nuire. Sa motivation peut être criminelle.

**White Hat**: Hacker qui pénètre dans un système informatique avec l'objectif principal d'aider le propriétaire à mieux le sécuriser.

**Grey Hat**: Hacker qui peut tout aussi bien aider à sécuriser les systèmes qu'à réaliser des exploits aux conséquences plus néfastes.

\* \* \*

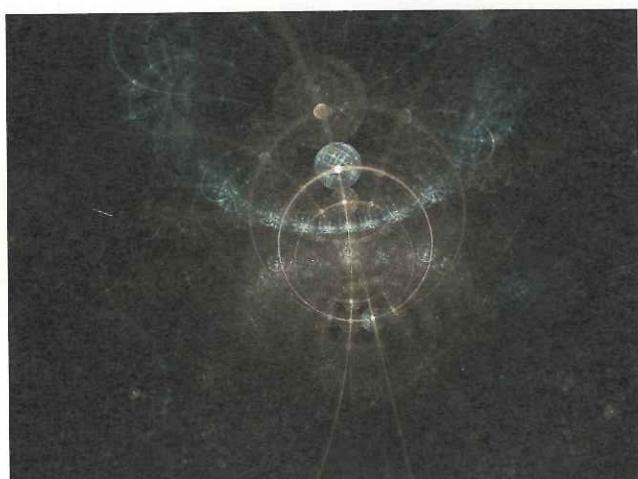
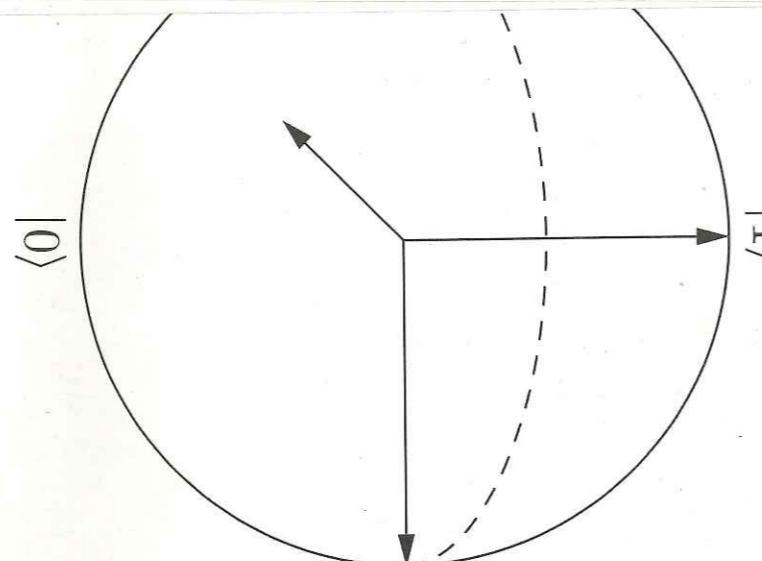
Chapeau noir, chapeau blanc, chapeau gris



## LES DIFFÉRENTES COUCHES DU WEB

Et s'il existait une partie du web inconnue des utilisateurs et des moteurs de recherche ? Une contrée inexplorée, des milliards de pages inaccessibles ? À la manière d'un iceberg, le web de tous les jours se compose de plusieurs couches :

- Le « surface web » ou web visible est la partie du web accessible à tous et consultable par les moteurs de recherche.
- Le « deep web », ou web invisible est la partie du web qui n'est pas consultable car non indexée par les moteurs de recherche. Comme ceux-ci n'y ont pas accès, les utilisateurs ne peuvent les consulter.
- Le « dark web », « dark net » ou le web de l'ombre, est un sous-ensemble du web invisible. Parce qu'il est chiffré, l'anonymat y est presque garanti pour les utilisateurs, les hébergeurs, et les détenteurs de ressources web. Parmi diverses technologies, l'utilisation du réseau « TOR » (« The Onion Router » ou



## DÉCLARATION D'INDÉPENDANCE DU CYBERESPACE

Rédigée le 8 février 1996 à Davos en Suisse par John Perry Barlow, l'un des fondateurs de l'Electronic Frontier Foundation, la Déclaration d'indépendance du cyberspace soutient l'idée qu'aucun gouvernement (ou qu'aucune autre forme de pouvoir) ne peut s'imposer et s'approprier Internet, alors en pleine extension. Elle a été écrite en partie en réponse à l'adoption de la Loi sur les télécommunications de 1996 aux Etats-Unis. Elle témoigne de l'esprit de liberté et de contre-culture quelques années seulement après la création du World Wide Web en 1989.



## CRYPTOGRAPHIE ET ADN

inquiète. Tous les pirates informatiques ne sont pourtant pas des cybercriminels. Si le cyberspace rendu anonyme peut être le lieu de la délinquance numérique, il peut aussi être celui de la défense des droits humains, de l'accès aux savoirs, de la créativité artistique, de la protection de la vie privée... Pour y voir plus clair, laissez-vous guider dans les profondeurs du dark web ! ■

inquiète. Tous les pirates informatiques ne sont pourtant pas des cybercriminels. Si le cyberspace rendu anonyme peut être le lieu de la délinquance numérique, il peut aussi être celui de la défense des droits humains, de l'accès aux savoirs, de la créativité artistique, de la protection de la vie privée... Pour y voir plus clair, laissez-vous guider dans les profondeurs du dark web ! ■



# QU'EST-CE QUE LA CRYPTOGRAPHIE ?

La cryptographie est l'une des deux disciplines qui composent la science ou l'art de protéger l'information appelée la **cryptologie**, l'autre étant la **stéganographie**. Alors que la stéganographie a pour but de cacher l'existence d'un message (par exemple en utilisant de l'encre sympathique), la **cryptographie** rassemble les techniques visant

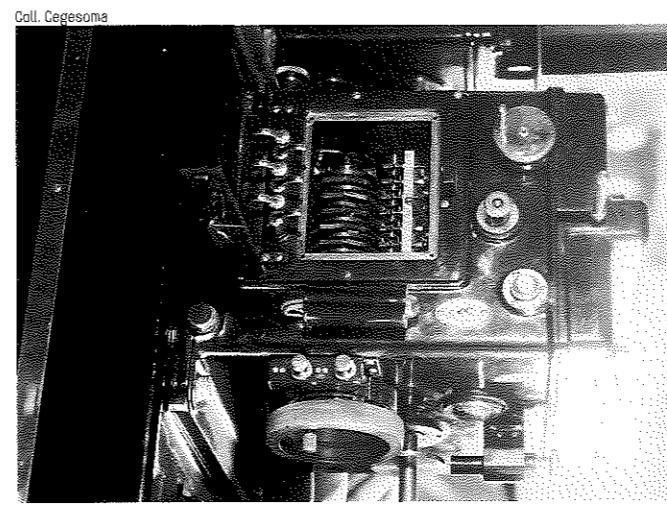
à cacher le contenu d'un message ou d'une information en le chiffrant, c'est-à-dire en le rendant illisible pour quine dispose pas de la clé pour le déchiffrer.

Le chiffrement d'un texte dit « clair » (visible partout) utilise deux techniques. La première est la **substitution**, qui peut se faire de deux manières :

- en remplaçant un mot par un autre mot, un chiffre ou un symbole au moyen d'un **code** établi (simplifiant l'usage d'un répertoire de mots de code);
- en remplaçant une lettre par une autre lettre, un chiffre ou un symbole dans une méthode précise, appelée **chiffre**, plus ou moins complexe (par exemple en utilisant un ou plusieurs alphabets).

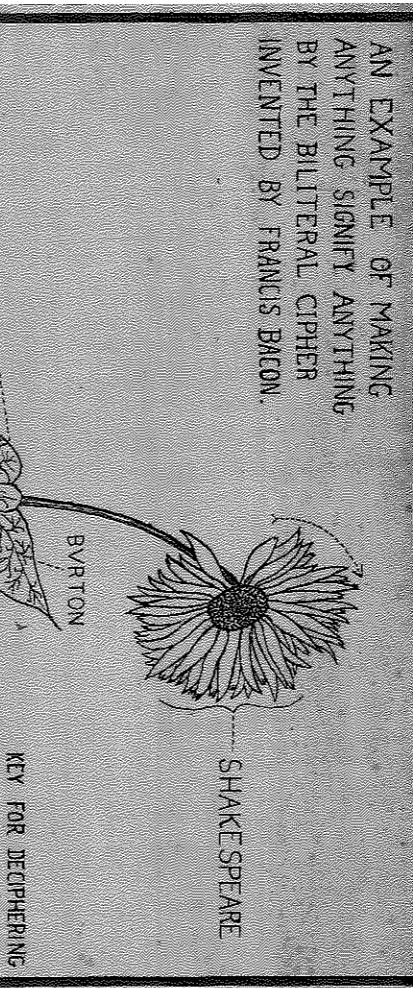
La deuxième technique est la **transposition** consistant à changer la place d'une lettre, d'un chiffre ou d'un symbole dans un message.

Un **cryptogramme** (une information chiffrée) est le résultat d'un **algorithme**, c'est-



Coll. Cegesoma

▲ Cryptographe Bélin, [années 1930]



KEY FOR DECRYPTING

LETTERING IN

LEGEND:

**A** — = a

**B** — = b

**C** — = c

**D** — = d

**E** — = e

**F** — = f

**G** — = g

**H** — = h

**I** — = i

**J** — = j

**K** — = k

**L** — = l

**M** — = m

**N** — = n

**O** — = o

**P** — = p

**Q** — = q

**R** — = r

**S** — = s

**T** — = t

**U** — = u

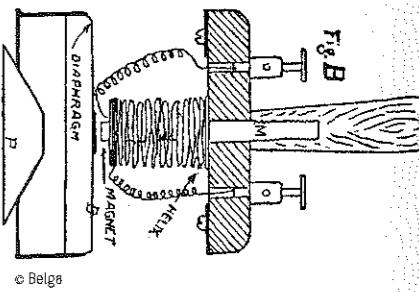
**V** — = v

**W** — = w

**X** — = x

**Y** — = y

**Z** — = z



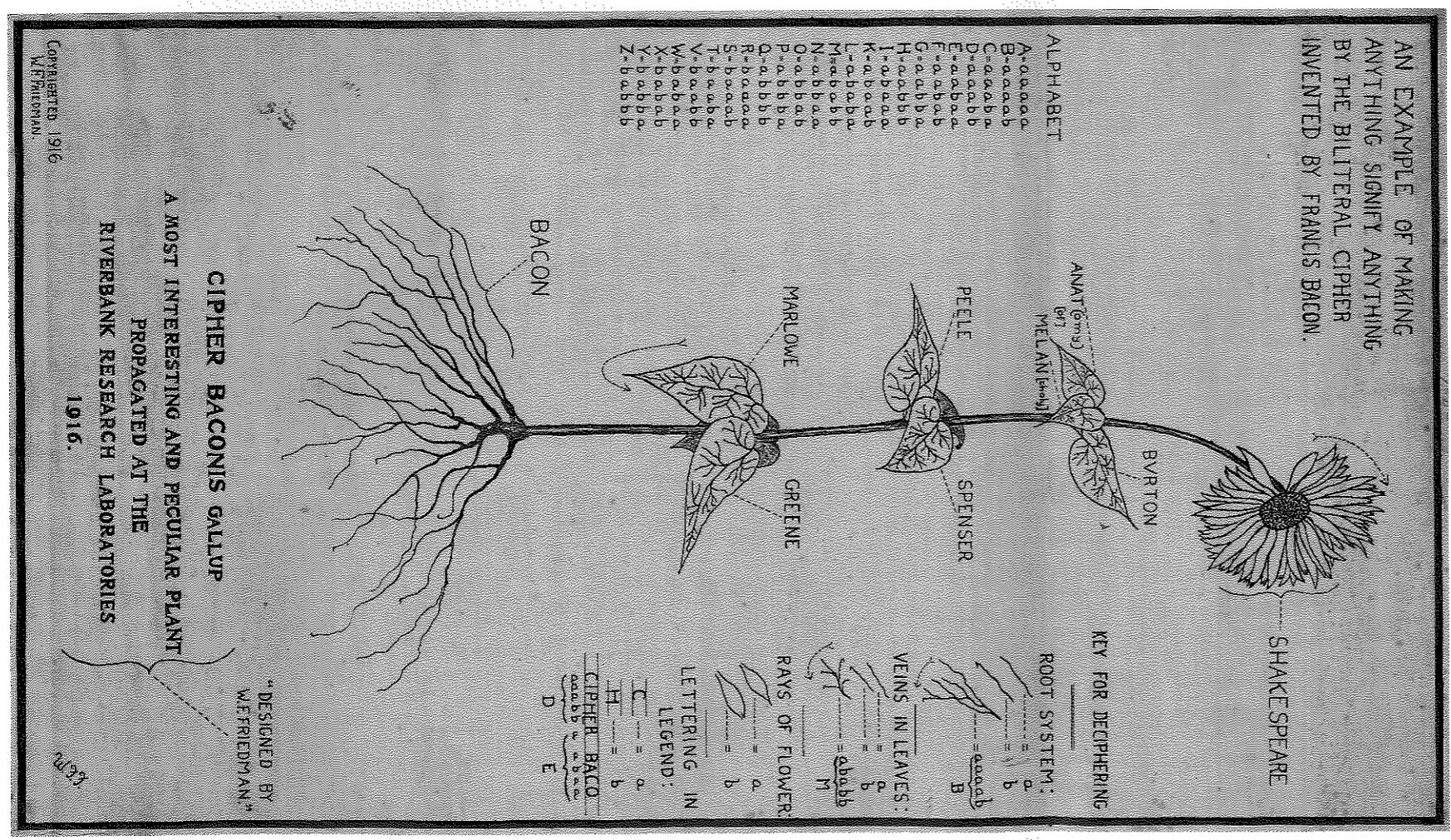
© Belgia

à dire d'une suite d'opérations mêlant souvent ces deux techniques. Cette « récette » est réalisée manuellement jusqu'au début du 20<sup>e</sup> siècle, ensuite par des outils mécaniques ou électromécaniques (les machines que sont les **cryptographes**), enfin par des moyens électroniques et informatiques.

Un cryptogramme ne peut en théorie être déchiffré qu'avec la clé de déchiffrement correspondant à l'algorithme utilisé. Un moyen de tester la fiabilité d'un algorithme est de le mettre à l'épreuve de la **cryptanalyse**, la discipline consistant à déchiffrer un cryptogramme sans disposer de la clé. ■

Le philosophe anglais Francis Bacon (1561-1626) est l'inventeur d'un système stéganographique qu'il appelle l'alphabet binaire. Ce système consiste à remplacer les lettres de l'alphabet par des arrangements des lettres A et B en groupes de 5.

▼



Copyright © 1916

W.Friedman

1916.

Coll. New York Public Library

Depuis l'Antiquité, l'éventail est utilisé pour se rafraîchir par temps chaud. Cet usage est bien connu mais l'on sait moins qu'il a également servi à communiquer au moyen d'un langage codé.

## LE LANGAGE DE L'ÉVENTAIL

Depuis l'Antiquité, l'éventail est utilisé pour se rafraîchir par temps chaud. Cet usage est bien connu mais l'on sait moins qu'il a également servi à communiquer au moyen d'un langage codé.

## KAMASUTRA (5<sup>e</sup> siècle)

Première description de cryptage par substitution. Parmi les arts que les femmes doivent maîtriser figure celui de l'écriture secrète (qui doit leur permettre de dissimuler leurs liaisons). L'une des techniques conseillées consiste à apposer au hasard les lettres de l'alphabet et à substituer ensuite dans le message original la nouvelle lettre de la paire à celle d'origine.

## CIPHER BACONIS GALLUP

A MOST INTERESTING AND PECULIAR PLANT  
PROPAGATED AT THE  
RIVERBANK RESEARCH LABORATORIES



## PROPRIÉTÉS DE LA CRYPTOGRAPHIE

La cryptographie s'attache à protéger les messages en se basant sur trois concepts.

### LA CONFIDENTIALITÉ

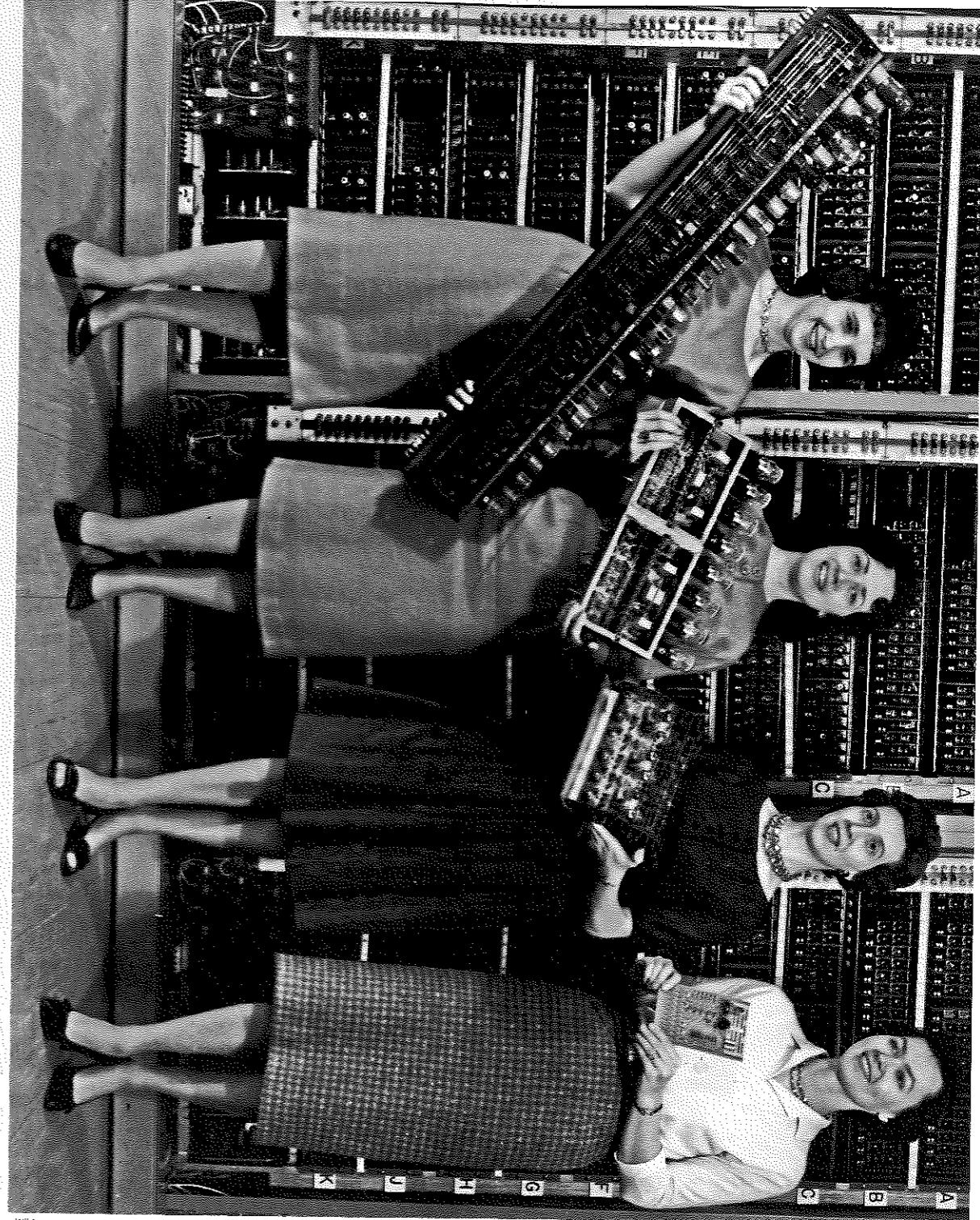
Elle permet de garder secret le contenu d'un message grâce au chiffrement (comme s'il était placé dans un coffre fermé à clé).

### L'INTÉGRITÉ

Elle permet de s'assurer que le message n'a pas été modifié lorsque le destinataire le reçoit. Ce principe, particulièrement important dans le domaine de l'information, est assuré par des garanties telles que la signature numérique, souvent renforcée par le tatouage (stéganographie).

### L'IDENTIFICATION OU L'AUTHENTIFICATION

Elle permet de s'assurer de l'identité de l'expéditeur du document, notamment grâce au scelllement (message chiffré puis signé).



Wikicommons

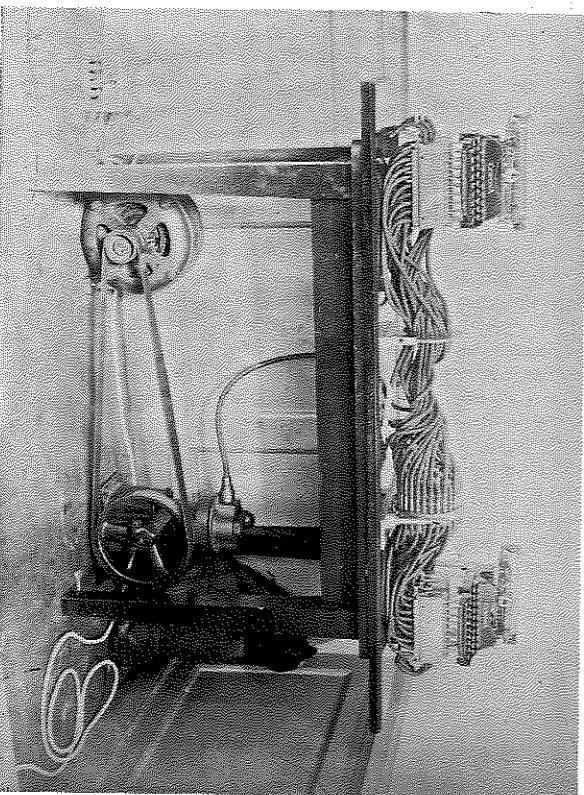
# À QUOI LA CRYPTOGRAPHIE SERT-ELLE ?

Historiquement, la cryptographie a été développée à des fins d'abord militaires ou étatiques. Dès l'Antiquité, les armées ont souhaité, en temps de guerre, pouvoir échanger des messages sans que l'ennemi ne puisse les intercepter. De même, le souci de confidentialité a poussé les États et leurs services secrets à imaginer des systèmes de chiffrement de plus en plus sophistiqués. La machine Enigma, créée en 1918, est sans doute l'appellation la plus célèbre de ce besoin. La cryptographie a également servi à garder le secret de complots, ou encore de découvertes économiques ou scientifiques. Par exemple, Galilée utilisait des anagrammes pour décrire ses découvertes astrologiques afin d'en garder la primeur.

Le développement des moyens de communication depuis l'apparition des premiers télégraphes et téléphones au 19 siècle, a accru la nécessité de sécuriser les infor-

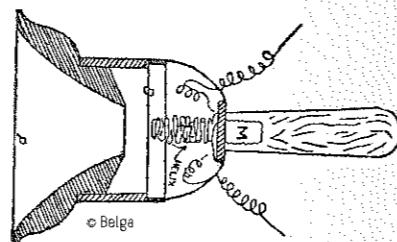
mations échangées : quand un moyen de communication offre la possibilité de capter le contenu émis, la cryptographie s'avère nécessaire pour protéger les informations sensibles. De nos jours, l'explosion de l'informatique, d'Internet et de la téléphonie mobile a rendu la cryptographie omniprésente dans notre quotidien,

sans même que nous en ayons conscience. De la carte à puce de nos cartes bancaires aux applications mobiles, du paiement en ligne au vote électronique, de la protection de nos données privées au tatouage des images numériques, la cryptographie est partout. Elle est devenue un outil incontournable. ■



Coll. Bibliothèque nationale de France

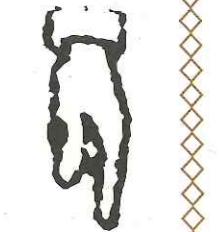
Dispositif permettant d'écrire en Morse



### MANUSCRIT DE VOYNICH

Ce livre manuscrit et illustré est découvert en 1912 par Wilfrid M. Voynich dans une communauté de jésuites près de Rome. Il daterait du début du 15<sup>e</sup> siècle et est écrit dans un alphabet à ce jour encore indéchiffré, malgré les nombreuses tentatives des cryptographes.





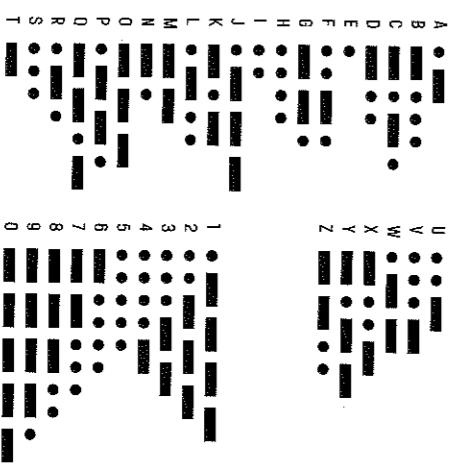




ZIGZAG: — — — — —

### LE CHIFFREMENT PAR PIQUE DÉPINLES

Ce procédé est imaginé dans la Grèce antique par l'historien Phèle le Tacticien. Il consiste à percer de trous minuscules le papier d'un message apparemment anodin, composant un message qui sera déchiffré par le destinataire. Dans les années 1850, cette méthode est encore utilisée, l'envoi de journaux n'étant pas taxé, certains utilisent cette méthode pour éviter d'envoyer des lettres.



13 - 34 - 14 - 15: — — —

### 3.

— — / — — / . . . / . . . / .

Le morse fait correspondre à chaque lettre ou chiffre une combinaison de signaux courts ou longs. Ce code, inventé par Samuel Morse pour la télégraphie, peut être transmis par des sons, des signaux lumineux, des traits et des points, etc.

ALIAS:

— — / . / . . . — / — . . / . . . / . . .

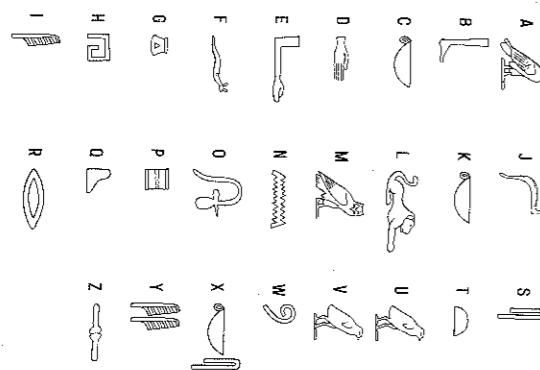
### 5.

#### ÉCRITURE EN MIROIR

Certains, comme le peintre et inventeur de la Renaissance Léonard de Vinci, parviennent à écrire à l'envers, de droite à gauche. Un moyen rapide de cacher un message... mais facile à décoder avec un miroir!

MINAUT: — — — — —

BUTELLE: — — — — —

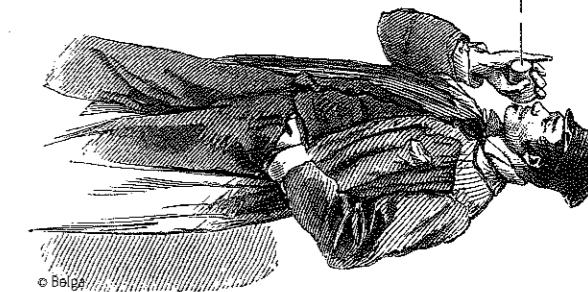
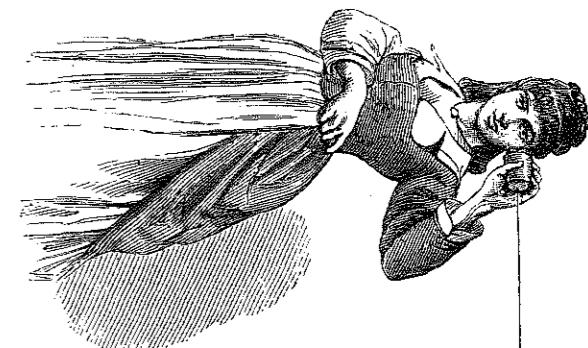


1	2	3	4	5	6
2	A	B	C	D	E
3	F	G	H	I/J	K
4	L	M	N	O	P
5	Q	R	S	T	U
6	V	W	X	Y	Z

Le mathématicien, historien et écrivain grec Polybe (2<sup>e</sup> 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.

#### CARRÉ DE POLYBE



© Belga

### 2.

#### CHIFFRE DE CÉSAR

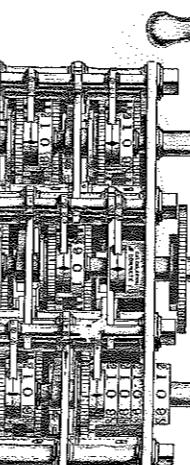
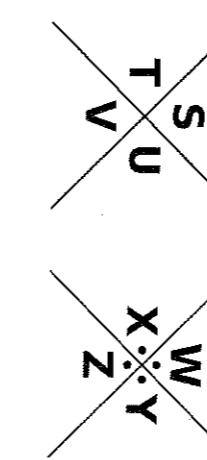
Le général romain Jules César (1<sup>er</sup> siècle avant notre ère) codait ses messages en remplaçant chaque lettre par celle qui se situe 3 places plus loin dans l'alphabet. On peut aussi utiliser une roue pour voir quelle lettre correspond au message original.

CESAR: — — — — —

KRWHO: — — — — —

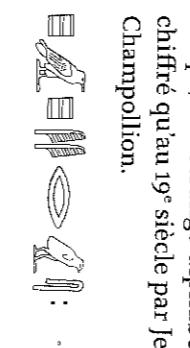
MORSE: — — — — —

A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R



### 6.

Durant l'Antiquité, les Égyptiens avaient une écriture originale : les hiéroglyphes. Des dessins représentaient des sons, qui formaient des mots. Oublié pendant longtemps, cet étrange alphabet ne fut déchiffré qu'au 19<sup>e</sup> siècle par Jean-François Champollion.



### 4.

#### LA CRYPTOGRAPHIE ET LA MUSIQUE CLASSIQUE

L'alphabet du parc à cochons ou *Pigpen*, est un code associant un symbole à chaque lettre, d'après un système de grilles et de points. Il a été inventé par les Francs-maçons au 17<sup>e</sup> siècle.

© Belga

— < — — — — < —

— — — — — — —

— — — — — — —



