Les codes secrets décryptés

3ème édition corrigée et augmentée
avec 45 cryptogrammes

Didier Müller

4EL .CH

Nymphomath Éditions

version 3.0 : 9 septembre 2018
version 3.7 : 31 décembre 2025

ISBN 978-2-8399-2485-6

À Pierre Baud

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve... »

« On peut affirmer que l'ingéniosité humaine ne peut pas élaborer un chiffre que l'ingéniosité humaine ne peut résoudre... »

Edgar Allan Poe

A Few Words on Secret Writing, 1841.

AVANT-PROPOS

La cryptologie, plus communément appelée la science des codes secrets, est à la fois une science et un art. C'est une science, car elle fait appel aux mathématiques et à l'informatique, que ce soit pour chiffrer des messages ou pour les décrypter. La cryptologie est aussi un art, car elle fait appel aux talents d'intuition, d'imagination et d'invention du décrypteur, ces facultés étant elles-mêmes secondées par des connaissances linguistiques approfondies.

Je voulais écrire un livre qui s'inscrirait dans la ligne de ceux des grands cryptologues du 20ème siècle : **Baudouin**, **Friedman**, **Givierge**, **Langie**, **Sacco**, **Fouché Gaines, Sinkov**, et quelques autres. Leurs livres ne se contentaient pas de présenter des systèmes de chiffrement, ils montraient aussi leurs faiblesses et comment les décrypter.

Je vous invite donc à un voyage dans le temps, depuis l'Antiquité jusqu'à nos jours, où vous découvrirez les systèmes de chiffrement qui ont marqué leur époque. Nous regarderons plus d'une centaine de chiffres, la plupart ne demandant que du papier et un crayon. Plus nous avancerons dans ce livre, et plus les systèmes de chiffrement deviendront complexes.

Au chapitre 11, je ne ferai qu'effleurer la cryptographie moderne, car elle fait appel à des notions mathématiques et informatiques très complexes, que j'essaierai de simplifier au maximum. On peut faire l'impasse sur ce chapitre ou se référer à la bibliographie si on veut en savoir plus.

Les codes secrets ne sont pas l'apanage des militaires et des diplomates. Des auteurs célèbres, férus de cryptographie – comme **Edgar Allan Poe**, **Jules Verne**, **François Rabelais, Arthur Conan Doyle** - ont écrit des romans où le décryptement d'un message secret jouait un rôle central. En les étudiant de près, nous verrons à quel point ces textes sont réalistes. Des sculpteurs, peintres, dessinateurs, politiques s'amusent aussi avec les codes secrets. Nous verrons quelques exemples amusants.

La deuxième édition de ce livre a paru en 2011. Depuis, j'ai appris moult nouvelles choses et découvert d'autres passionnés sur le web, notamment le cryptologue et auteur allemand **Klaus Schmeh** qui tenait un blog fantastique sur le sujet : « Cipherbrain » (malheureusement fermé depuis 2023). Tout cela m'a donné envie de reprendre la plume (ou plutôt le clavier) et d'améliorer la deuxième édition. De plus, je voulais écrire un e-book, qui permet de faire des mises à jour fréquentes, d'améliorer sans frais l'iconographie, et de se passer d'intermédiaires. De plus, d'un simple clic, on peut consulter d'autres documents intéressants qui complètent le propos.

Cette troisième édition est en effet un « e-book augmenté ». Vous trouverez au fil des pages des « QR codes » ressemblant à ceci :

Vous pourrez cliquer sur ce QR code si vous lisez ce livre sur un support numérique. Vous pourrez ainsi tester les codes secrets que vous trouverez dans ce livre.

Si vous avez préféré imprimer cet e-book, il vous faudra installer sur votre smartphone une application qui lit les QR codes. Vous pointerez ensuite un QR code avec la caméra de votre appareil pour accéder à la page web qui vous permettra d'essayer le système de chiffrement présenté.

Dans cette troisième édition, je voulais aussi rendre hommage à **Pierre Baud**, mon ami cryptologue qui nous a quittés en 2014. Quelques passages de cet e-book ont été écrits par lui.

Par rapport aux livres de mes glorieux prédécesseurs, la grande originalité de celui-ci est d'être couplé avec un site web dont l'adresse est :

www.apprendre-en-ligne.net/crypto

J'ai commencé ce site en 2001 déjà, avec l'intention d'en faire un cours en ligne pour mes élèves de lycée. Le sujet est tellement passionnant que ce site a grandi, grandi... et trouvé son aboutissement dans cet e-book, après deux éditions imprimées.

Remerciements

Je tiens à remercier ici ceux qui m'ont inspiré pour cet e-book, soit par leurs publications ou leurs travaux, soit par la correspondance que j'ai entretenue avec eux.

Tout d'abord trois de mes élèves qui ont réalisé sous ma direction des « travaux de maturité » remarquables dans le domaine de la cryptographie : **Jan Jungfer**, **Sven Reber** et **Matteo Zuber**.

Ensuite les cryptologues que j'ai croisés dans la vraie vie ou au hasard du web : **Frédéric Bayart**, **Pierre Baud**, **Elonka Dunin**, **Jean Louis Fritsch** (alias Gielev), **George Lasry**, **Hervé Lehning**, **Jean-Louis Morel** (alias Rossignol), **Sébastien Peronno**, **Dirk Rijmenants** et **Klaus Schmeh**.

Conventions

Dans la plupart des livres, les lettres d'un message codé sont en majuscules, celle d'un message clair en minuscules. J'ai aussi adopté cette convention.

Sauf exceptions, les messages clairs ne contiennent pas de lettres accentuées, ni d'espaces, ni de signes de ponctuation. On ne chiffrera donc que les lettres de *a* à *z*.

Traditionnellement, on regroupe les lettres d'un cryptogramme par groupes de cinq, car ainsi le nombre de lettres se compte plus rapidement. D'autre part, on complique la tâche du casseur de code en ne respectant pas les espaces entre les mots du clair.

J'utiliserai des abréviations du style [ABCD12] pour les références à un livre de la bibliographie, où « ABCD » sont, en principe, les quatre premières lettres de l'auteur et « 12 » les deux derniers chiffres de l'année de parution du livre.

La numération des pages vous étonnera peut-être. J'écrirai d'abord le numéro du chapitre, suivi du numéro de la page dans ce chapitre. Par conséquent, la première page de chaque chapitre *C* aura le numéro *C*-1. Je pourrai ainsi facilement modifier un chapitre sans me préoccuper des autres. En effet, cet e-book va évoluer avec le temps : il est prévu de faire une mise à jour chaque fin d'année, entre octobre et décembre.

Table des matières

1

INTRODUCTION

« On a inventé l'art d'écrire avec des chiffres ou avec des caractères inconnus pour dérober la connaissance de ce qu'on écrit à ceux qui interceptent des lettres, mais l'industrie des hommes, qui s'est raffinée par la nécessité & l'intérest, a trouvé des règles pour déchiffrer ces lettres & pour pénétrer par ce moyen dans les secrets d'autruy. »

François de Callières (1645 – 1717)

1.1. Définitions de termes courants

Avant tout, il faut définir certains termes couramment utilisés en cryptologie, mais qui sont si spécifiques qu'on ne les trouve pas forcément dans les dictionnaires !

Algorithme
Suite d'opérations élémentaires à appliquer à des données pour aboutir à un résultat désiré. Par exemple, une recette de cuisine est un algorithme.

Antigramme
Texte déjà chiffré qui va être **surchiffré**.

Asymétrique
Un chiffrement est asymétrique s'il utilise une clef pour chiffrer un message et une autre clef pour le déchiffrer.

Attaque
Tentative de **décryptement**.

Bigramme
Séquence de deux lettres consécutives. Adjectif : bigrammique (bigrammatique dans certains ouvrages). Exemples: ee, th, ng, ...

Casser
Dans l'expression « casser un code », trouver la clef ou l'algorithme de chiffrement.

Chiffre
Manière secrète d'écrire un message à transmettre, au moyen de caractères et de signes disposés selon une convention convenue au préalable. Les deux grandes familles de chiffres sont les **substitutions** et les **transpositions**.

Chiffrement
Opération qui consiste à transformer un texte clair en **cryptogramme**. On parle de « chiffrement » car à la Renaissance, on utilisait principalement des chiffres arabes comme caractères de l'écriture secrète.

Clair (ou message clair)
Version intelligible d'un message.

Clef
Dans un système de **chiffrement**, elle correspond à un nombre, un mot, une phrase, etc., qui permet, grâce à l'**algorithme** de **chiffrement**, de **chiffrer** ou de **déchiffrer** un message.

Code
1. Système de symboles permettant d'interpréter, de transmettre un message, de représenter une information, des données.
2. Sorte de dictionnaire qui à un mot (ou une phrase) fait correspondre un groupe de lettres ou de chiffres. Par exemple, « aujourd'hui » = E4WYQ

Cryptanalyse
Art d'analyser un message chiffré afin de le **décrypter**. On parle aussi de **décryptement**.

Cryptogramme
Message écrit à l'aide d'un système de **chiffrement**.

Cryptographie (du grec κρυπτος : caché et γραφειν : écrire)
Art de transformer un message clair en un message inintelligible pour celui qui ne possède pas les clefs de **chiffrement**. Cependant, on utilise souvent le mot **cryptographie** comme synonyme de **cryptologie**.

Cryptologie
(du grec κρυπτος : caché et λογος : science)
Science des messages secrets. Elle se décompose en deux disciplines : la **cryptographie** et la **cryptanalyse**.

Déchiffrement
Opération inverse du **chiffrement**. Opération qui consiste à obtenir la version originale d'un message qui a été précédemment chiffré en connaissant la méthode de **chiffrement** et les **clefs** (contrairement au décryptement).

Décryptement
Opération qui consiste à retrouver le clair sans disposer des clefs théoriquement nécessaires. Il ne faut pas confondre **déchiffrement** et **décryptement**.

Double clef (chiffre à)
Synonyme de chiffre **polyalphabétique**.

Monoalphabétique
Se dit d'un chiffre où une lettre du message **clair** est toujours remplacée par le même symbole. On parle aussi de substitution simple.

Monogramme
Une lettre ou un symbole. Adjectif : **monogrammique**. Cet adjectif est peu utilisé. Il s'oppose à polyalphabétique. Quand on parle de substitution monoalphabétique, il est sous-entendu.

Nomenclateur
Méthode de chiffrement qui contient à la fois des éléments d'un code (définition 2) et d'un chiffre.

Nulles
Symboles sans signification rajoutés dans un message pour certains **algorithmes**. On les emploie soit pour compléter un message de manière à atteindre une certaine longueur, soit pour tromper ceux qui cherchent à **décrypter** le message en noyant les informations utiles au milieu de caractères, mots ou phrases inutiles.

Polyalphabétique
Se dit d'un **chiffre** où plusieurs alphabets de **chiffrement** sont utilisés en même temps. Une lettre n'est plus chiffrée par un seul symbole, mais par plusieurs différents.

Polygramme
Séquence de *n* lettres ou symboles. Adjectif : **polygrammique**.

Polygrammique
Se dit d'un chiffre où un groupe de *n* lettres est chiffré par un groupe de *m* symboles. Souvent $n = m$. On ne chiffre donc pas des lettres mais des **polygrammes**.

Répertoire
Table mettant en correspondance un code (par exemple un nombre, mais cela peut aussi être un mot) et sa signification.
Exemple :

12	Les navires ennemis sont au port
341	Pape
442	Roi
8755	Nous demandons des renforts

Sémagramme
Dans un sémagramme, les éléments du texte codé ou chiffré ne sont ni des lettres, ni des chiffres : le sens est véhiculé par différents éléments, par exemple des points de jetons de dominos, l'emplacement d'objets sur une image, etc.

Simple
Synonyme de **monoalphabétique**.

Stéganographie
(du grec στεγανος : couvert et γραφειν : écrire)
Branche particulière de la **cryptographie** qui consiste non pas à rendre le message inintelligible, mais à le camoufler dans un support (une texte, une image, les mailles d'un tricot, etc.) de manière à masquer sa présence.

Substitution
Un chiffre de substitution remplace les caractères du message en clair par des symboles (caractères, nombres, signes, etc.) définis à l'avance.

Surchiffrement
Chiffrement d'un message déjà chiffré par une autre méthode.

Symétrique
Un chiffrement est symétrique s'il utilise la même clef pour chiffrer et déchiffrer un message.

Tétragramme
Séquence de quatre lettres consécutives.
Exemples : eche, this, pong, ...

Tomogrammique
Dans les systèmes tomogrammiques, chaque lettre est tout d'abord représentée par un groupe de plusieurs symboles ; ces symboles sont ensuite chiffrés séparément ou par groupes de taille fixe.

Transposition
Un chiffre de transposition ne modifie pas les caractères mais les mélange selon une méthode prédéfinie.

Trigramme
Séquence de trois lettres consécutives.
Exemples : ehe, thi, ong, …

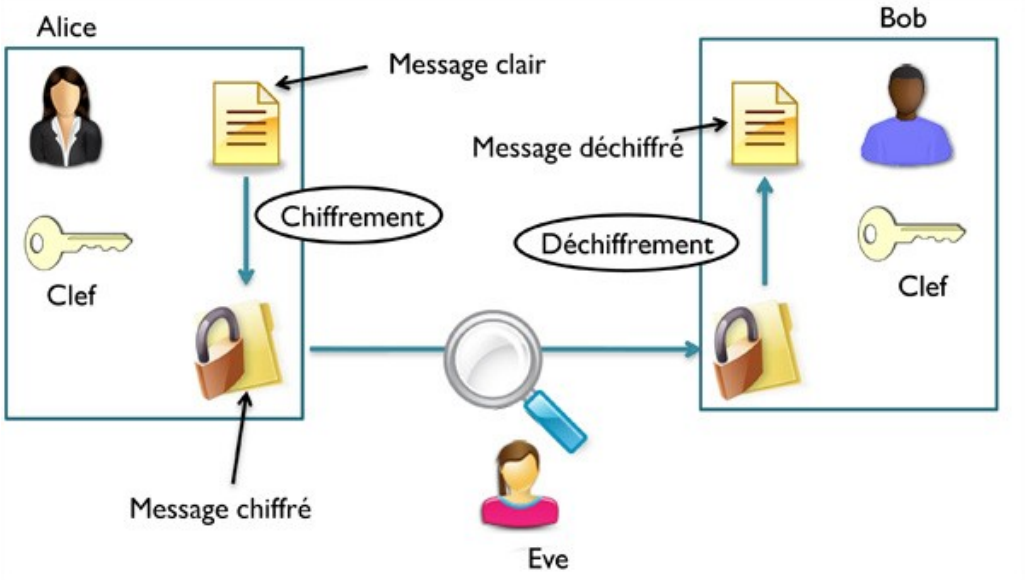
1.2. Alice et Bob

Les personnages d'**Alice et Bob** sont des figures classiques en cryptologie. Ces noms sont utilisés au lieu de « personne A » et « personne B » ; Alice et Bob cherchent dans la plupart des cas à communiquer de manière sécurisée.

Ces noms ont été inventés par **Ron Rivest** pour son article de 1978 dans le *Communications of the ACM* qui présentait le cryptosystème RSA.

Si d'autres protagonistes participent aux échanges, on les appellera **Carol(e)**, puis **Dave**.

Il existe beaucoup d'autres personnages, mais le plus important dans mon livre sera , une écouteuse externe (de l'anglais *eavesdropper*). C'est une attaquante *passive* : elle peut écouter les échanges d'Alice et de Bob, mais elle ne peut pas les modifier.

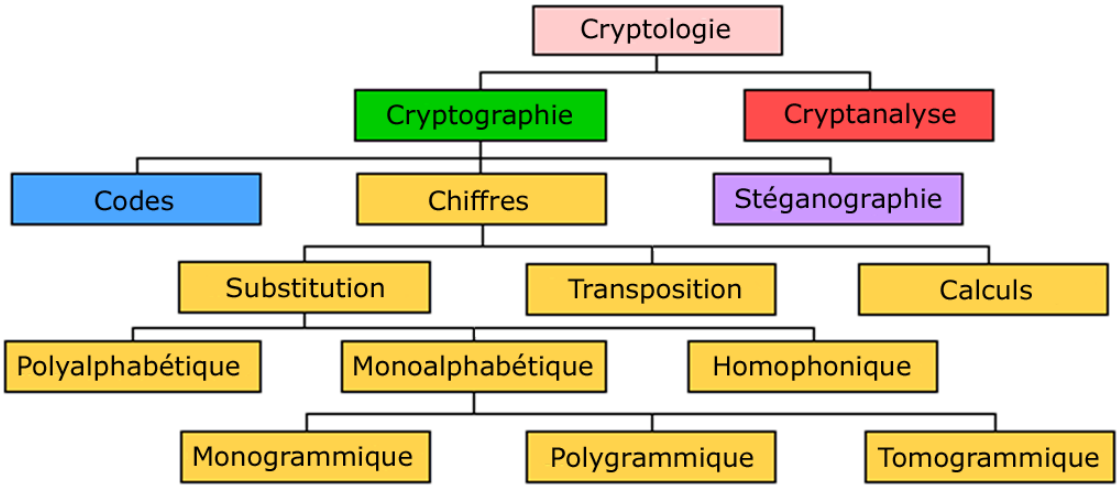


Mallory (ou *Mallet*, pour *malicieux*), est un attaquant *actif*. Au contraire d'Eve, Mallory peut modifier les messages, substituer les siens, remettre en jeu d'anciens messages, etc. Rendre un système sûr vis-à-vis de Mallory s'avère un problème plus difficile que pour Eve. Ces problèmes d'a*uthentification* et d'*intégrité* ne seront pas abordés dans ce livre.

Vous trouverez une liste complète des personnages de la cryptologie sur la page Wikipédia *Alice et Bob*.

1.3. Classification des systèmes de chiffrement

Les différents systèmes de chiffrement peuvent être classés selon le schéma ci-dessous :



1.4. Repères historiques

Les 3000 premières années (de 2000 av. J.-C. à 1000 ap. J.-C.)

Les écritures secrètes semblent être nées spontanément dès que, dans une région, une partie importante de la population savait lire.

Environ 1900 avant J.-C.		Un scribe égyptien emploie des hiéroglyphes non conformes à la langue correcte dans une inscription. L'historien spécialiste de la cryptographie **David Kahn**[1] le qualifie de premier exemple documenté de cryptographie écrite.
Environ 1500 av. J.-C.		Une tablette mésopotamienne contient une formule chiffrée pour la fabrication de vernis pour les poteries. Un potier y avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots.
600-500 avant J.-C.		Des scribes hébreux mettant par écrit le livre de Jérémy ont employé un simple chiffre de substitution connu sous le nom d' « Atbash ». C'était un des chiffres hébreux de cette époque.
487 av. J.-C.		Les Grecs emploient un dispositif appelé la *scytale* - un bâton autour duquel une bande de cuir longue et mince était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager. Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message.
Environ 150 avant J.-C.		L'historien grec **Polybe** (env. 200-125 av. J.-C.) invente le « carré de Polybe », dont s'inspireront plus tard bien d'autres cryptosystèmes.

[1] voir [KAHN96] dans la bibliographie

60-50 avant J.-C.		**Jules César** (100-44 avant J.-C.) emploie une substitution simple avec l'alphabet normal (il s'agissait simplement de décaler les lettres de l'alphabet d'une quantité fixe) dans les communications du gouvernement. Ce chiffre n'est pas robuste, mais à une époque où très peu de personnes savent lire, cela suffit. César écrit aussi parfois en remplaçant les lettres latines par les lettres grecques.
5ème siècle ?		On trouve dans le *Kama-sutra* le *mlecchita-vikalpa*, l'art de l'écriture secrète, qui doit permettre aux femmes de dissimuler leurs liaisons.
8ème siècle		**al-Khalil ibn Ahmad** (718-786), grammairien, écrit le livre *Kitab al-Mu'amma* (le livre des messages cryptographiques). Il y traite de la méthode du mot probable.
855		**Abu Bakr ben Wahshiyya** publie plusieurs alphabets secrets utilisés à des fins de magie, dans son livre *Kitab shauk almustaham fi ma'arifat rumuz al aklam*.
9ème siècle		**Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi** (801-873) rédige le plus ancien texte connu décrivant la technique de décryptement appelée « analyse des fréquences ».
Vers 1200		**Ali ibn'Adlān** (1187-1268) est né à Mossoul et est surtout connu pour ses contributions précoces à la cryptanalyse à laquelle il a consacré plus d'un livre. Ses deux ouvrages majeurs sur la cryptanalyse étaient *Al-mu'lam* et *Al-mu'allaf lil-malik al-'Asraf*. L'une de ses contributions les plus importantes portait sur la taille du texte pour l'utilisation de l'analyse des fréquences.
Vers 1200		Le poète et cryptologue arabe **Ibn Dunaynir** (1187-1229) décrit pour la première fois un procédé de chiffrement faisant appel à un calcul dans son livre *Maqasid al-Fusul al-Mutarjamah an Hall at-Tarjamah*.

L'éveil de l'Occident (de 1200 à 1800)

Jusque-là largement devancé par la science arabe, l'Occident développe la cryptographie et la cryptanalyse.

1226		À partir de 1226, une timide cryptographie politique apparaît dans les archives de Venise : des points ou des croix remplacent les voyelles dans quelques mots épars.
Environ 1250		**Roger Bacon** décrit plusieurs chiffres. Il écrit : « Il est fou celui qui écrit un secret de toute autre manière que celle qui le soustrait à la connaissance du vulgaire ».

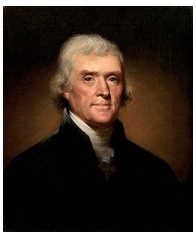
Environ 1350		**Ali ibn Muḥammad Ibn al-Durayhim** (1312-1361) était un cryptologue arabe qui a donné des descriptions détaillées de huit systèmes de chiffrement qui ont discuté des chiffres de substitution , menant à la première suggestion d'un tableau qui deux siècles plus tard est devenu célèbre sous le nom de « carré de Vigenère » Son livre intitulé *Effacer les objectifs des chapitres et résoudre les problèmes* a récemment été découvert, mais il n'a pas encore été publié. Il comprend l'utilisation des techniques statistiques mises au point par Al-Hindi et Ibn ‘Adlan.
1379		**Gabriele de Lavinde** compose un recueil de clefs, dont plusieurs combinent code et substitution simple. En plus d'un alphabet de chiffrement, souvent avec des nulles, on trouve un petit répertoire d'une douzaine de noms communs et de noms propres avec leurs équivalents en bigrammes. C'est le premier exemple d'un procédé qui prévaudra pendant 450 ans en Occident : le « nomenclateur »
1412		La science arabe en matière de cryptologie est exposée dans la *subh al-a sha*, une énorme encyclopédie en 14 volumes, écrite pour fournir à la bureaucratie une connaissance exhaustive de toutes les principales branches du savoir. Son auteur, qui vit en Égypte, est **Abd Allah al-Qalqashandi**. La section intitulée *De la dissimulation des informations secrètes dans les lettres* comporte deux parties, l'une traitant des représentations symboliques et du langage convenu, l'autre des encres invisibles et de la cryptologie.
1466-67		**Leon Battista Alberti** invente et publie le premier chiffre polyalphabétique. Il conçoit un cadran chiffrant pour simplifier le processus. Cette classe de chiffre n'a pas été cassée jusqu'aux années 1800. Alberti écrit aussi largement sur l'état de l'art dans des chiffres. Ces chiffres polyalphabétiques sont beaucoup plus robustes que le nomenclateur qu'utilisent les diplomates de l'époque. Alberti invente aussi le surchiffrement codique.
1474		**Sicco Simonetta**, cryptanalyste au service du Duc de Milan, écrit *Liber Sifrorum*, un traité de cryptanalyse.
1506		Le premier grand cryptanalyste européen est peut-être **Giovanni Soro**, qui devient secrétaire du Chiffre de Venise en 1506. Le Vatican lui-même teste ses chiffres sur Soro, qui les perce à jour une première fois.
1518		Le premier livre imprimé sur la cryptologie est publié deux ans après la mort de son auteur, **Jean Trithème**. Cet abbé invente un chiffre stéganographique dans lequel chaque lettre est représentée par un mot. Le résultat ressemble à une prière. Il décrit aussi des chiffres polyalphabétiques sous la forme désormais standard de tables de substitution rectangulaires.

Environ 1550		**Jérôme Cardan** invente le premier procédé autoclave, mais ce système est imparfait, et c'est finalement un autre procédé qui porte son nom : « la grille de Cardan » (voir § 2.3).
1553		**Giovan Batista Bellaso** fait paraître un petit livre intitulé *La cifra del. Sig. Giovan Batista Bellaso*. Il y propose, pour le chiffrement en substitution polyalphabétique, l'emploi de clefs littérales, faciles à garder en mémoire et à changer. Il les appelle « mots de passe ». Les clefs littérales sont immédiatement adoptées et l'innovation de Bellaso est à l'origine de certains systèmes actuels très complexes où plusieurs clefs - et non pas une seule - sont utilisées et changées de façon irrégulière.
1563		**Giovanni Battista Della Porta** écrit *De Futivis Literarum Notis*. Ces quatre livres, traitant respectivement des chiffres anciens, des chiffres modernes, de la cryptanalyse et des caractéristiques linguistiques qui favorisent le déchiffrement, représentent la somme des connaissances cryptologiques de l'époque. Parmi les procédés modernes, dont beaucoup sont de son invention, apparaît la première substitution bigrammique : deux lettres sont représentées par un seul symbole. Il invente aussi le premier chiffre polyalphabétique. Il est le premier à classer les deux principes cryptographiques majeurs : la substitution et la transposition.
1578		**Marins**, un des décrypteurs de la République de Venise, fait paraître *Del mondo di extrazar le cifre*.
1585		**Blaise de Vigenère** écrit son *Traicté des chiffres ou secrètes manières d'escrire*. Il présente entre autres un tableau du type Trithème, que l'on dénomme aujourd'hui à tort « carré de Vigenère ».
1623		Sir **Francis Bacon** (que l'on soupçonne par ailleurs fortement d'être William Shakespeare) est l'inventeur d'un système stéganographique qu'il expose dans *De dignitate et augmentis scientiarum*. Il appelle son alphabet « bilitère », car il utilise un arrangement des deux lettres A et B en groupes de cinq.
1641		**John Wilkins**, évêque de Chester, publie anonymement *Mercury, or the Secret and Swift Messenger*, le premier livre anglais sur la cryptographie.
1665		Le scientifique et jésuite allemand **Gaspar Schott** publie son ouvrage Schola steganographica.

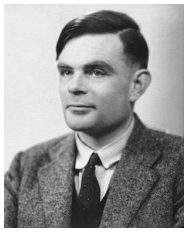
1691		**Antoine Rossignol** et son fils **Bonaventur**e élaborent le « Grand Chiffre de Louis XIV » qui tombera en désuétude avec la mort de ses inventeurs, et ses règles précises seront rapidement perdues. Le Grand Chiffre est si robuste qu'on sera incapable de le lire, jusqu'à ce qu'**Étienne Bazeries** réussisse à la casser.

L'essor des communications (de 1800 à 1970)

Les nouvelles techniques de communications (moyens de transports rapides, journaux, télégraphe, télégraphie sans fil) donnent une nouvelle impulsion à la cryptologie. Pour la première fois de l'histoire de l'humanité, une parole va plus vite qu'un messager à cheval. La transmission d'un message se libère du transport. Forcément, les guerres modernes utilisent abondamment les télécommunications ; l'interception devient simple et le décryptement des informations devient vital. La cryptologie entre dans son ère industrielle.

Environ 1790		**Thomas Jefferson**, futur président des États-Unis, invente son cylindre chiffrant, si bien conçu qu'après plus d'un siècle et demi de rapide progrès technique, il sera encore utilisé. C'est certainement le moyen de chiffrement le plus sûr de l'époque, et pourtant il sera classé et oublié. Il sera réinventé en 1891 par **Étienne Bazeries**, qui ne parviendra toutefois pas à le faire adopter par l'armée française.
1854		**Charles Wheatstone**, un des pionniers du télégraphe électrique, invente le chiffre Playfair, du nom de son ami **Lyon Playfair** qui popularisera ce chiffre.
1854		**Charles Babbage** casse le chiffre de Vigenère, mais sa découverte reste ignorée, car il ne la publie pas. Ce travail ne sera mis en lumière qu'au 20ème siècle, lors de recherches effectuées sur l'ensemble des papiers de Babbage. Cependant, il ne publie pas ses travaux et cette avancée importante dans l'histoire de la cryptanalyse est attribuée au Polonais **Friedrich Kasiski** en 1863.
1857		Après la mort de l'amiral Sir **Francis Beaufort**, son frère publie le « chiffre de Beaufort » (une variante du chiffre de **Vigenère**).
1859		**Pliny Earl Chase** publie dans *Mathematical Monthly* la première description d'un chiffre tomogrammique.

1863		Le major polonais **Friedrich W. Kasiski** publie *Die Geheimshriften und die Dechiffrierkunst* (les chiffres et l'art du déchiffrement), qui donne la première solution générale pour le déchiffrement d'un chiffre polyalphabétique à clef périodique, marquant ainsi la fin de trois siècles d'invulnéra-bilité du chiffre de Vigenère.
1883		Le Hollandais **Auguste Kerckhoffs** publie *La cryptographie militaire*. Il y expose notamment quelques règles à respecter pour concevoir un bon système cryptographique, toujours valables actuellement, dont la principale est la suivante : la sécurité d'un système ne doit pas reposer sur le secret de la méthode de chiffrement.
1891		Le commandant **Étienne Bazeries** produit son cryptographe cylindrique. Il était composé de vingt disques portant chacun vingt-cinq lettres. Il ne sera jamais employé par l'armée française. Bazeries fut aussi le premier à déchiffrer le Grand chiffre de Louis XIV.
1917		Le télégramme Zimmermann, intercepté en 1917 par le Royaume-Uni qui décrypta son contenu, a accéléré l'entrée en guerre des États-Unis.
1917		**Gilbert S. Vernam**, travaillant pour AT&T, invente une machine de chiffre polyalphabétique pratique capable d'employer une clef qui est totalement aléatoire et ne se répète jamais - un « masque jetable ». C'est le seul chiffre dont on a prouvé qu'il était indécryptable en pratique et en théorie. Ce procédé ne sera cependant jamais utilisé par l'armée car il exige de devoir produire des millions de clefs différentes (une par message), ce qui est impossible en pratique. Par contre, il sera utilisé par les diplomates allemands dès 1921.
1918		Le système ADFGVX est mis en service par les Allemands à la fin de la première guerre mondiale. Il sera cassé par le lieutenant français **Georges Painvin**.
1918		**Arthur Scherbius** fait breveter sa célèbre machine à chiffrer *Enigma*. Notons que trois autres inventeurs, dans trois pays, ont, chacun de leur côté et presque simultanément, l'idée d'une machine basée sur des rotors : **Hugo Alexandre Koch** (Pays-Bas, 1870-1928), **Arvid Gerhard Damm** (Suède, 1869-1927) et **Edouard Hugh Hebern** (États-Unis, 1869-1952). 

1925		**Boris Caesar Wilhelm Hagelin** (1892-1983) propose à l'armée suédoise la machine B-21, qui sera pendant une décennie la machine la plus compacte capable d'imprimer des messages chiffrés. Pendant la seconde guerre mondiale, les Alliés fabriquèrent une autre machine de Hagelin, la Hagelin C-36 (appelée M-209 aux États-Unis), à 140'000 exemplaires. Après la guerre, Boris Hagelin créera à Zoug, en Suisse, Crypto AG.
1929		**Lester S. Hill** publie son article *Cryptography in an Algebraic Alphabet*, dans *American Mathematical Monthly*, 36, 1929, pp. 306-312. Il y décrit le chiffre qui porte son nom. C'est un chiffre polygraphique où l'on utilise des matrices et des vecteurs.
1931		**Herbert O. Yardley** publie *The American Black Chamber*, un des livres les plus célèbres sur la cryptologie. Avant cela, il avait décrypté entre autres les codes japonais (avant leur machine PURPLE).
1933-45	 	La machine *Enigma* n'est pas un succès commercial (son prix a découragé de nombreux acheteurs potentiels) mais elle est reprise et améliorée pour devenir la machine cryptographique de l'Allemagne nazie. Elle est cassée par le mathématicien polonais **Marian Rejewski**, qui s'est basé seulement sur un texte chiffré et une liste des clefs quotidiennes obtenues par un espion. Pendant la guerre, les messages sont régulièrement décryptés par **Alan Turing** et d'autres à Bletchley Park, en Angleterre, à l'aide des premiers ordinateurs (les fameuses « bombes »).
1940		**William Frederick Friedman**, plus tard honoré comme le père de la cryptanalyse américaine, à la tête de son équipe du Signal Intelligence Service (S.I.S.), réussit le décryptement de la machine de cryptage japonaise PURPLE. Avec sa femme, il s'intéressera beaucoup aux chiffres shakespeariens.

La cryptologie moderne (de 1970 à nos jours)

Les ordinateurs et le réseau Internet font entrer la cryptologie dans son ère moderne. La grande invention de ces dernières décennies est la cryptographie à clef publique. Le futur sera peut-être la cryptographie quantique, définitivement indécryptable.

1970		Au début des années 1970, **Horst Feistel**, un des premiers cryptographes universitaires, mène un projet de recherche à l'IBM Watson Research Lab et développe le chiffre *Lucifer*, qui inspirera plus tard le chiffre DES et d'autres algorithmes de chiffrement symétrique par blocs.
1973-74		Divers articles classifiés secrets ont été rédigés au GCHQ pendant les années 1960 et 1970 et ont finalement conduit à des algorithmes essentiellement identiques au chiffrement RSA, quelques années avant la publication des universitaires américains. Les inventeurs (**James Ellis**, **Clifford Cocks** et **Malcolm Williamson**) n'ont été connus que plus tard, secret défense oblige.
1976		**Whitfield Diffie** et **Martin Hellman** publient *New Directions in Cryptography*, article qui introduit l'idée de cryptographie à clef publique. Ils donnent une solution entièrement nouvelle au problème de l'échange de clefs. Ils avancent aussi l'idée d'authentification à l'aide d'une fonction à sens unique. Ils terminent leur papier avec une observation intéressante : « L'habileté dans la cryptanalyse a toujours été lourdement du côté des professionnels, mais l'innovation, en particulier dans la conception des nouveaux types de systèmes cryptographiques, est venue principalement d'amateurs. »
Novembre 1976		DES, pour Data Encryption Standard (en français : standard de cryptage de données), est un algorithme très répandu à clef privée dérivé du chiffre *Lucifer* de **Feistel** dans sa version à 64 bits. Il sert à la cryptographie et l'authentification de données. Il est jugé si difficile à percer par le gouvernement des États-Unis qu'il est adopté par le Ministère de la Défense des États-Unis, qui contrôle depuis lors son exportation. Cet algorithme a été étudié intensivement et est devenu l'algorithme le mieux connu et le plus utilisé dans le monde à ce jour.
Avril 1977 1978	  	RSA signifie Rivest-Shamir-Adleman, en l'honneur de ses trois inventeurs : **Ron Rivest**, **Adi Shamir** et **Leonard Adleman**, (ci-contre, de haut en bas) qui l'ont inventé en 1977. Le brevet de cet algorithme appartient à la société américaine *RSA Data Security*, qui fait maintenant partie de *Security Dynamics*, et aux *Public Key Partners* (PKP à Sunnyvale, Californie, États-Unis), qui possèdent les droits en général sur les algorithmes à clef publique. RSA est un algorithme à clef publique qui sert aussi bien à la cryptographie de documents qu'à l'authentification. Comme il est très sûr, l'algorithme RSA est devenu un standard *de facto* dans le monde. L'algorithme RSA est publié dans les *Communications de l'ACM*.

1990		**Xuejia Lai** et **James Massey** publient *A Proposal for a New Block Encryption Standard*, un algorithme de cryptage des données International (l'IDEA : International Data Encryption Algorithm) - pour remplacer le DES. L'IDEA emploie une clef de 128 bits et utilise des opérations convenant bien à tout type d'ordinateurs, permettant donc une programmation plus efficace. Il s'agit d'un des meilleurs algorithmes de chiffrement, si ce n'est le meilleur. Personne n'a déclaré à ce jour avoir cassé d'une manière ou d'une autre le moindre bloc de texte chiffré par IDEA. Il est actuellement exploité par la société *Mediacrypt*.
1990		**Charles H. Bennett** et **Gilles Brassard** publient leurs résultats expérimentaux sur la cryptographie quantique, qui emploie des photons pour communiquer un flot de bits qui serviront de clefs pour un cryptage de type **Vernam** (ou d'autres utilisations). En supposant que les lois de la mécanique quantique se vérifient, la cryptographie quantique offre non seulement le secret, mais permet aussi de savoir si la ligne a été écoutée.
1991		**Philip Zimmermann** sort sa première version de PGP (Pretty Good Privacy) en réponse à la menace du FBI d'exiger l'accès au message clair des citoyens. PGP offre une haute sécurité au citoyen, et cela gratuitement. Cela lui valut une enquête criminelle de trois ans de la part des Douanes américaines, au prétexte d'avoir violé les restrictions sur l'exportation de logiciels de cryptographie en diffusant PGP dans le monde entier (PGP avait été publié en 1991 sur le web comme logiciel libre). Sous l'influence des banques (ayant besoin de protéger les données communiquées aux clients), la procédure fut classée sans suite début 1996.
Août 1999		11 sites répartis dans 6 pays factorisent le premier nombre ordinaire de 155 chiffres décimaux (512 bits). Un tel nombre aurait pu servir de clef dans un système de chiffrement moderne de type RSA, qui est utilisé dans le commerce électronique. Un tel record remet en question l'utilisation de clefs trop petites dans de tels systèmes.
2000		*Rijndael* a été conçu par **Joan Daemen** et **Vincent Rijmen**, deux chercheurs belges, dans le but de devenir un candidat à l'*Advanced Encryption Standard* (AES) du NIST (National Institute of Standards and Technology). *Rijndael* a été choisi comme standard en 2000, prenant la place du premier véritable standard de la cryptographie : le DES.
2007		L'équipe du professeur genevois **Nicolas Gisin** bat son propre record (18 km) en répétant l'expérience Bernex-Bellevue de 1997, qui montrait que l'intrication quantique était conservée sur plusieurs kilomètres dans des fibres optiques télécom. Les résultats ont été publiés dans la revue *Nature* du 18 août 2008.

2009		L'un des acteurs majeurs du développement des chiffrements homomorphes, **Craig Gentry**, publie sa thèse intitulée « *A Fully Homomorphic Encryption Scheme* ».

1.5. Références

Livres

[BAUC13] Bauer Craig P., **Secret History: The Story of Cryptology**, Chapman and Hall/CRC, 2013

[KAHN80] Kahn David, **La guerre des codes secrets**, InterEditions, 1980

[KAHN96] Kahn David, **The Codebreakers, The Story of Secret Writing**, Revised Edition, Scribner, 1996

[LEHN19] Lehning Hervé, **La Bible des codes secrets**, Flammarion, 2019

[NEWT98] Newton David E., **Encyclopedia of Cryptology**, ABC-CLIO, 1998

[PRAT40] Pratt Fletcher, **Histoire de la cryptographie**, Payot, Paris, 1940

[SING99] Singh Simon, **Histoire des codes secrets**, LC Lattès, 1999

Sites

- Ellison Carl, « Cryptography Timeline », <http://world.std.com/~cme/html/timeline.html>
- Sale Tony, « The 1944 Bletchley Park Cryptographic Dictionary », <http://www.codesandciphers.org.uk/documents/cryptdict/cryptix.htm>
- Wikipédia, « Histoire de la cryptologie », <https://fr.wikipedia.org/wiki/Histoire_de_la_cryptologie>
- Wikipédia, « Liste de cryptologues », <https://fr.wikipedia.org/wiki/Liste_de_cryptologues>
- Wikipédia, « Alice et Bob », <https://fr.wikipedia.org/wiki/Alice_et_Bob>

2

STÉGANOGRAPHIE

Contrairement à la cryptographie proprement dite qui *transforme* des messages de manière à les rendre incompréhensibles, la stéganographie (en grec « l'écriture couverte ») *cache* les messages dans un support. Peut-être connaissez-vous cette série de livres-jeux pour enfants, *Où est Charlie ?,* édités par **Martin Handford**, où un personnage dessiné est à retrouver dans une foule compacte ? C'est une forme de stéganographie : le personnage est là et bien reconnaissable, mais il est caché dans la masse. Où est-il ?

On peut faire la distinction entre cryptographie et stéganographie ainsi :

Cryptographie : texte visible mais incompréhensible.
Stéganographie : texte compréhensible mais invisible.

Évidemment, rien n'empêche de combiner les deux...

Les premiers emplois attestés de la stéganographie se lisent chez **Hérodote** vers le 5ème siècle avant Jésus-Christ : un certain **Histiée**, voulant prendre contact secrètement avec son gendre, le tyran **Aristagoras de Milet**, choisit un esclave dévoué, lui rasa la tête, et y inscrivit le message à transmettre. Il attendit que ses cheveux repoussent pour l'envoyer à Aristagoras en lui ordonnant de se faire raser le crâne une fois sur place.

Toujours d'après Hérodote, pour informer les Spartiates de l'attaque imminente des Perses, un certain **Démarate** utilisa un élégant stratagème : il prit des tablettes, en racla la cire et grava sur le bois le message secret, puis il recouvrit les tablettes de cire.

En Chine ancienne, on écrivait les messages sur une fine soie dont on faisait une petite boule en l'englobant dans de la cire. Le messager avalait cette boule, qui était ensuite récupérée par les voies naturelles.

L'historien de la Grèce Antique **Énée le Tacticien** imagina envoyer un message secret en piquant de minuscules trous sous certaines lettres d'un texte anodin. La succession de ces lettres fournit le texte secret. Deux mille ans plus tard, les épistoliers anglais employèrent la même méthode, non pour assurer le secret à leurs envois, mais pour éviter de payer des taxes excessives. En effet, dans les années 1850, envoyer une lettre coûtait environ un shilling tous les cents miles, ce qui était hors de portée de la plupart des gens, mais les journaux ne payaient pas de taxe. Grâce aux piqûres d'épingles, les plus malins pouvaient envoyer leurs messages gratuitement. Ce procédé a été aussi utilisé par les Allemands pendant la Première Guerre Mondiale. Au cours de la Seconde Guerre Mondiale, ils améliorèrent le procédé en cochant les lettres de journaux avec de l'encre sympathique.

Au 16ème siècle, le scientifique italien **Giovanni Battista Della Porta**, une grande figure de la cryptographie, découvrit comment cacher un message dans un œuf dur : il suffit d'écrire sur la coquille avec une encre contenant une once d'alun pour une

pinte de vinaigre ; la solution pénètre la coquille et dépose sur la surface du blanc d'œuf le message qu'on lira aisément après avoir épluché l'œuf.

Un texte apparemment innocent peut aussi révéler un message important. Voici un exemple d'un tel message, envoyé par un espion allemand pendant la Seconde Guerre Mondiale :

> Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Si l'on prend la deuxième lettre de chaque mot, le message suivant émerge :

> Pershing sails from NY June 1.

Dans la série télévisée *Prison break*, diffusée en 2005, le héros Michael Scofield se fait arrêter pour être incarcéré dans la même prison que son frère, afin de le faire évader. Avant cela, il a pris soin de faire tatouer sur tout son corps les plans de la prison, camouflés dans des motifs de style gothique. Le dos contient tous les passages souterrains, et le torse une vue aérienne de la prison. D'autres tatouages plus petits, toujours bien intégrés dans l'ensemble, sont des aide-mémoire. Par exemple, le tatouage ci-contre fait référence à une vis dont Michael a besoin : Allen Schweitzer 11121147. Sous ce nom étrange se cache la marque d'une vis et son numéro de série. Elle sera nécessaire à Michael pour dévisser les boulons des toilettes de sa cellule. Le point du "i" de « Schweitzer » est un hexagone. Michael devra limer la vis jusqu'à ce qu'elle corresponde à la forme indiquée.

Terminons ce tour d'horizon par cette dépêche du jeudi 27 avril 2006 :

> **Da Vinci Code - Message codé dans le verdict**
> LONDRES. Le juge anglais qui a présidé récemment un procès en plagiat concernant le best-seller planétaire Da Vinci Code a tacitement reconnu jeudi avoir dissimulé un message codé dans les 71 pages de son très sérieux verdict. « Je ne peux pas commenter le jugement, mais je ne vois pas pourquoi rendre un jugement ne pourrait pas être aussi l'occasion de s'amuser », a déclaré Peter Smith, magistrat de la Haute Cour de Londres. Le juge, en rendant son verdict le 7 avril, avait estimé que le « Da Vinci Code » n'était pas un plagiat. Il avait rejeté les accusations de deux Britanniques selon lesquels son auteur avait repris le thème central d'un de leurs livres paru 20 ans plus tôt. Des lettres en italique dans les sept premiers paragraphes du verdict forment l'expression « Smithy Code », allusion au nom du juge. D'autres lettres en italique sont dispersées tout au long du verdict, sans que l'on puisse à première vue comprendre leur signification. « Cela ne semble pas être des fautes de frappe, vous ne trouvez pas ? », a ironisé Peter Smith, se bornant à dire qu'il confirmerait qu'il s'agit d'un message codé lorsqu'il aura été entièrement déchiffré, « ce qui n'est pas très difficile à faire ». La plaisanterie de ce magistrat de 54 ans semble être une première dans l'histoire judiciaire. « Le fait que quelques lettres soient en italique dans le texte n'affecte en rien le jugement », a commenté un porte-parole de la magistrature. (AP)

En effet, tout au long du jugement, long de 71 pages et que l'on peut trouver sur Internet, des lettres en italique sont clairement visibles. Mises bout à bout, cela donne « s m i t h y c o d e - j a e i e x t o s t[1] g p s a c g r e a m q w f k a d p m q z v z ». Le mystère sera résolu le lendemain 28 avril déjà, par l'avocat Dan Tench. Il a découvert que la partie incompréhensible du texte avait été chiffrée avec un système que nous verrons au § 7.7 et qui se nomme « la variante allemande du chiffre de Beaufort ». La clef de chiffrement

[1] Le juge a fait une erreur dans son chiffrement. Ce *t* devrait être un *h*. Il a apparemment glissé au moment de mettre une lettre en italique puisqu'il a écrit « *t*he » au lieu de « t*h*e ».

était la suite de Fibonacci légèrement modifiée[2] pour une raison obscure : 1, 1, 25, 3, 5, 8, 13, 21, et qui correspond à la clef littérale AAYCEHMU[3].

Le message décodé n'est pas beaucoup plus explicite : « Jackie Fisher who are you ? Dreadnought » (en français : « Qui es-tu Jackie Fisher ? Dreadnought »). Le malicieux juge Smith, qui a confirmé que c'était bien le message caché, est décrit dans le *Who's who ?* comme un grand admirateur de John « Jackie » Fisher, un amiral du 19ème siècle qui est considéré comme le modernisateur de la marine britannique avec le développement du premier navire de guerre moderne, le « Dreadnought ». Dans un message électronique, le magistrat a expliqué qu'il avait introduit cette référence dans le jugement car l'ouverture du procès du *Da Vinci Code* avait coïncidé à peu près avec le 100ème anniversaire du baptême du navire.

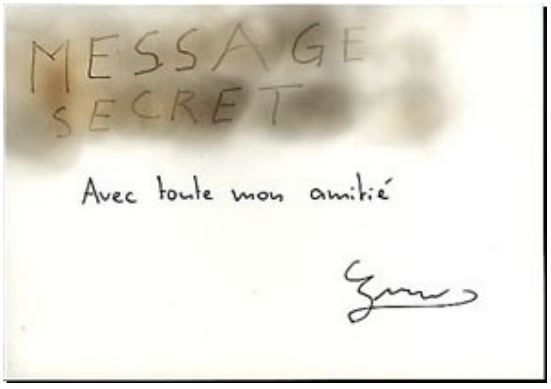
2.1. Encres invisibles

Les encres invisibles (on les qualifie aussi de *sympathiques*) sont les piliers centraux de la stéganographie.

Encres apparaissant avec le feu

- Différents acides, ou les sucs de différents fruits ;
- le jus de citron donnera une couleur brune ;
- le jus de cerise une couleur verdâtre ;
- celui d'oignon une couleur noirâtre ;
- l'acide vitriolique, affaibli dans une assez grande quantité d'eau, une couleur rousse ;
- le vinaigre, une couleur rouge pâle.

Le lait peut aussi constituer une excellente encre sympathique. Vous écrivez tout d'abord votre message anodin sur une simple feuille de papier (assez épaisse) et vous tracez ensuite les mots secrets sur la feuille en utilisant un cure-dent imprégné de lait. Vous laissez sécher (absorbez le surplus de lait avec un papier buvard) : le message inscrit au lait est alors invisible. Ensuite, il suffit à votre destinataire de chauffer la feuille à l'aide d'une bougie pour que le message réapparaisse.



La technique précédente fonctionne aussi avec le citron. Pressez le jus d'un oignon avec quelques gouttes de jus de citron. Il suffit à votre destinataire de chauffer la feuille à l'aide d'une bougie pour révéler l'encre. Le problème du citron est que l'odeur facilement identifiable qui se dégage du message trahit la présence d'un message caché...

Le degré de chaleur pour faire apparaître les caractères écrits avec ces différents liquides n'est pas le même. Le jus de citron est celui qu'il faut le moins chauffer.

[2] La vraie suite est 1, 1, 2, 3, 5, 8, 13, 21, ... Chaque nombre est la somme des deux qui le précèdent. Cette suite joue un rôle important dans le roman *Da Vinci Code*.

[3] A=1, B=2, C=3, ..., Y=25, Z=26.

Encres apparaissant avec de la poudre

On peut tracer sur le papier des caractères invisibles avec tous les sucs glutineux et non colorés des fruits ou des plantes, ou bien avec la bière, l'urine, le lait des animaux, et toutes les différentes liqueurs grasses ou visqueuses. Lorsque cette écriture est séchée, on répand dessus de la poussière colorée très fine, on secoue le papier, et les caractères restent colorés. Il suffit par exemple de répandre du charbon tamisé très fin ou du bleu de Prusse.

On trouve la description d'un tel procédé dans l'*Art d'aimer*, d'**Ovide**, livre III, 627-630 :

> Tuta quoque est fallitque oculos e lacte recenti littera : carbonis puluere tange, leges.
> Fallet et umiduli quae fiet acumine lini,
> et feret occultas pura tabella notas.
>
> Elle est sûre aussi et trompe les yeux, la lettre faite de lait frais : saupoudre-la de poussière de charbon et tu liras. Elle trompera aussi, celle qui sera écrite avec la pointe humide d'une tige de lin, et la tablette intacte portera des caractères cachés.

Pline l'Ancien, dans son *Histoire naturelle*, Livre XXVI, Ch. XXXIX présente une technique similaire :

> Tithymallum nostri herbam lactariam vocant, alii lactucam caprinam, narrantque lacte eius inscripto corpore, cum inaruerit, si cinis inspergatur, apparere litteras, et ita quidam adulteras adloqui maluere quam codicillis.
>
> Les auteurs romains appellent le tithymale « herbe lactaire », d'autres « laitue caprine », et ils racontent que quand on a écrit sur un corps avec son lait, quand on le chauffe et si on y saupoudre de la cendre, les lettres apparaissent : c'est ainsi que certains préférèrent communiquer avec leur maîtresse de cette manière plutôt qu'avec des tablettes.

Encres utilisant des produits chimiques

- Une partie d'Eau-Blanche diluée dans cinq parties d'eau. Le développement se fait avec un tampon d'ouate imbibé d'un liquide épilatoire quelconque (contenant un sulfure).
- Un demi-cachet de laxatif au phénolphtaléine, deux cuillères à café d'ammoniaque et deux cuillères à dessert d'eau. Le développement se fait avec une solution de cristaux de soude dans l'eau.
- Une partie d'alun pour cent parties d'eau. Le développement est obtenu en repassant la feuille de papier avec un fer chaud.
- Solution diluée de chlorure de cuivre. Les caractères invisibles deviennent, à la chaleur, d'un beau jaune et disparaissent au fur et à mesure du refroidissement.
- Dissoudre du cuivre dans de l'acide chlorhydrique auquel on ajoute de l'acide nitrique. Les caractères apparaissent à la chaleur.
- Ajouter à une solution de nitrate de cobalt du nitrate de nickel. L'encre invisible devient verte en la chauffant.
- Écrire avec une solution aqueuse de chlorate de soude. Cette écriture n'apparaîtra qu'en passant sur l'encre sèche une petite éponge trempée dans une solution de vitriol de cuivre.
- Une partie d'eau forte avec trois parties d'eau. Tremper la feuille dans de l'eau ordinaire et tout sera visible.

Encres utilisant des fluides corporels

Les services secrets britanniques (MI6) ont découvert que le sperme pouvait servir d'encre invisible. Un journal d'un membre supérieur du Secret Intelligence Service (MI6) a révélé que pendant la Première Guerre mondiale, on a découvert que ce fluide corporel pouvait agir comme une encre invisible efficace.

En juin 1915, **Walter Kirke**, chef adjoint des renseignements militaires au *GQG* France, écrivait dans son journal que **Mansfield Cumming**, le premier chef (ou *C*) du *SIS* « faisait des recherches pour des encres invisibles à l'Université de Londres ».

En octobre, il a noté qu'il avait « entendu de *C* que la meilleure encre invisible était le sperme », qui ne réagissait pas aux principales méthodes de détection. De plus, il avait l'avantage d'être facilement disponible. Il fallait cependant rappeler aux agents d'utiliser uniquement de nouvelles réserves d'encre lorsque les correspondants commençaient à remarquer une odeur inhabituelle.

Ces révélations sont incluses dans le livre *MI6 : The History of the Secret Intelligence Service 1909-1949* par le professeur **Keith Jeffery**, paru en 2011.

2.2. Les Ave Maria de Trithème

L'abbé **Jean Trithème** (1462–1516) imagina vers 1500 un très astucieux système chiffré (les *Ave Maria*) comprenant une série de 14 alphabets dans lesquels les lettres étaient remplacées par des mots ou des groupes de mots. Chacun d'eux était choisi de manière telle qu'il résultait de leur succession un texte latin cohérent, ressemblant à une prière ou à une glorification religieuse. Des mots sans signification particulière étaient rajoutés pour articuler le texte, par exemple « oui ! » ou « mais ». **Trithème** décrit les *Ave Maria* dans le premier livre des *Polygraphiae* (1518), l'un des premiers livres connus traitant de cryptographie et de stéganographie. Voici l'un de ces alphabets :

A	dans les cieux	N	en Paradis
B	à tout jamais	O	toujours
C	un monde sans fin	P	dans la divinité
D	en une infinité	Q	dans la déité
E	à perpétuité	R	dans la félicité
F	sempiternel	S	dans son règne
G	durable	T	dans son royaume
H	sans cesse	U, V, W	dans la béatitude
I, J	irrévocablement	X	dans la magnificence
K	éternellement	Y	au trône
L	dans la gloire	Z	en toute éternité
M	dans la lumière		

Chiffrement

Chaque lettre du message est remplacée par une expression du tableau ci-dessus. Des mots de liaison sont insérés pour que la prière paraisse plus naturelle.

> Sempiternel dans la béatitude,
> Au trône à perpétuité,
> En toute éternité dans la béatitude,
> Oui ! toujours dans la béatitude.
>
> Dans son règne à perpétuité
> Et dans son royaume à perpétuité,
> Dans son règne dans une infinité.

À perpétuité dans un monde sans fin,
Toujours dans la béatitude,
Oui ! dans la béatitude à perpétuité.

Dans la félicité de son royaume,
Et dans son règne !

L'inconvénient du système réside dans le temps nécessaire à la transposition d'un texte de quelque importance et dans la grande taille du texte chiffré.

Déchiffrement

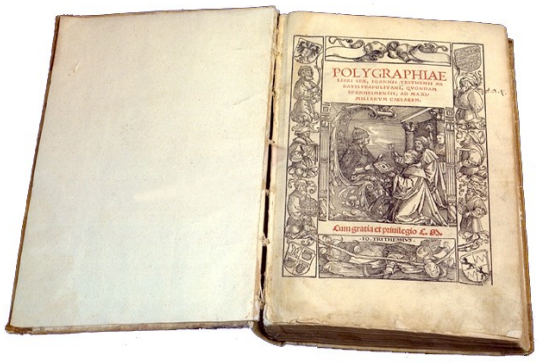
Pour déchiffrer, il suffisait de repérer dans la table de codage à quelle lettre correspond telle expression. La prière ci-dessus contenait le message caché « Fuyez ! Vous êtes découverts ».

Décryptement

Outre le fait que le message chiffré se présentait comme une suite normale de mots, les casseurs de code auraient dû, à cause des nombreuses équivalences, rechercher et accumuler une masse énorme de matériaux avant de parvenir à déceler des similitudes qui auraient pu leur permettre de reconstituer la table de codage.

Polygraphiae ne fut pas la première incursion de **Trithème** dans la cryptologie. En 1499, il avait composé un volume énigmatique et controversé appelé *Steganographia*. Pendant des années, il circula sous le manteau sous forme de manuscrit avant d'être finalement imprimé en 1606, puis inscrit dans la liste officielle des livres interdits en 1609. En apparence, il expliquait comment employer les esprits pour envoyer des messages secrets ! Les deux premiers livres de *Steganographia* contiennent de nombreux exemples de chiffres simples. Le livre III est largement composé de tables de nombres, dont les colonnes sont surmontées par des symboles zodiacaux et planétaires, suggérant des données astronomiques. Contrairement aux deux premiers livres, il y avait peu d'indices pour aider à déchiffrer le contenu. Il a finalement été décrypté indépendamment par **Thomas Ernst** en 1996 et **Jim Reeds** en 1998.

Johannes Trithemius



Polygraphiae (1518)

2.3. Grille de Cardan

Le procédé de la grille trouée semble avoir été inventé au 16ème siècle par **Jérôme Cardan** (1501−1576), médecin, mathématicien, astronome et philosophe italien de la Renaissance.

Chiffrement

La grille de Cardan consiste en une feuille d'un matériau rigide dans laquelle ont été découpées, à des intervalles irréguliers, des fenêtres rectangulaires de la hauteur d'une ligne d'écriture et de longueur variable.

Le chiffreur pose ce cache sur la feuille de papier et inscrit le message secret dans les fenêtres. Il enlève ensuite la grille et remplit les espaces vides avec des lettres quelconques.

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

Déchiffrement

Le déchiffreur place simplement la grille sur le texte pour voir apparaître le message.

■	■	C	■	■	■	■	E	■	■	■	■	T	A	■	■	■	I	■	■	■	■	T	■	■
A	■	■	■	M	E	G	■	■	A	■	■	■	R	■	■	A	■	■	F	■	■	A	■	U
B	O	■	■	■	■	■	U	■	■	R	G	■	■	D	■	■	■	E	■	C	■	A	R	■
■	■	■	T	H	■	■	■	A	■	■	■	G	■	E	■	■	D	■	■	A	N	■	■	S
L	■	■	E	■	■	S	■	J	A	■	■	■	■	■	R	■	■	■	D	■	I	■	N	■
■	S	■	■	D	H	A	■	■	■	M	■	■	I	■	■	L	■	■	■	C	■	A	R	■

Le message caché était donc :

« C'était à Mégara, faubourg de Carthage, dans les jardins d'Hamilcar. »

C'est la première phrase du roman *Salammbô*, de Gustave Flaubert. Nous retrouverons plusieurs fois des extraits de ce roman par la suite.

Variantes

Plutôt que de faire des trous pour des lettres, on peut aussi faire des trous pour des mots. On pourra ainsi camoufler un message dans une lettre anodine.

2.4. L'alphabet bilitère de Francis Bacon

Francis Bacon, Lord Verulam (1561–1626), est l'inventeur d'un système stéganographique qu'il mentionna d'abord en termes vagues dans un ouvrage paru en 1605 et intitulé *Of the proficience and advancement of Learning, divine and humane* (De la valeur de l'avancement de la science divine et humaine). Il l'exposa plus clairement en 1623 dans *De dignitate et augmentis scientiarum*.

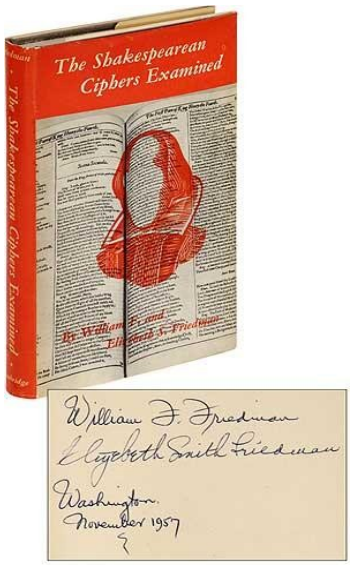
Le *baconisme* est la théorie selon laquelle Francis Bacon serait l'auteur des pièces de William Shakespeare. Plusieurs adeptes de cette théorie ont cherché

dans la grande édition de 1623 un code qui confirmerait cette thèse, mais en vain. **Elizabeth Wells Gallup** crut notamment y voir un chiffre bilitère, car elle trouvait que certaines lettres étaient légèrement différentes des autres ; elle publia ses résultats en 1899 dans un livre intitulé *The Bi-literal Cypher of Sir Francis Bacon in his works and Deciphered by Mrs Elizabeth Wells Gallup*.

Ce travail est très controversé. D'un côté les convaincus, de l'autre ceux qui crient à la supercherie.

Les travaux d'Elizabeth Wells Gallup sont âprement défendus par le **Général Cartier** qui donne des arguments assez convaincants du sérieux de la thèse, documents à l'appui, tout en reconnaissant que certains choix de Mrs Gallup sont difficiles à justifier.

Deux cryptologues américains, le fameux **William Friedman** et son épouse **Elizebeth** (photo ci-dessous prise en 1958), abordèrent scientifiquement le problème.



Dans *The Shakespearean Ciphers Examined*, ils réfutèrent les découvertes d'Elizabeth Wells Gallup (qui reconnaissait elle-même qu'une certaine dose d'« inspiration » était nécessaire à la reconnaissance des alphabets) : des agrandissements photographiques montrèrent que les différences entre caractères étaient dues le plus souvent à des déformations, des bavures d'encre ou des imperfections du papier.

Cette histoire est l'objet du livre du **Général Cartier** *Un problème de Cryptographie et d'histoire* [CART38].

Chiffrement

Francis Bacon commençait par remplacer les vingt-quatre lettres de l'alphabet de son temps (i se confondait avec j, et u avec v) par des arrangements des deux lettres A et B en groupes de cinq :

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

Alphabet bilitère de Bacon

Il est intéressant de constater que cet alphabet, que son inventeur appelait *alphabet bilitère*, est très semblable dans son principe au codage binaire de l'information dans nos ordinateurs actuels. Il suffit de remplacer les A par des 0 et les B par des 1.

L'alphabet chiffrant de Francis Bacon peut aussi s'écrire sous la forme d'un tableau de vingt-quatre cases (trois rangées de huit cases) dans lesquelles sont écrites les lettres de l'alphabet dans leur ordre normal :

	AAA	AAB	ABA	ABB	BAA	BAB	BBA	BBB
AA	a	b	c	d	e	f	g	h
AB	i-j	k	l	m	n	o	p	q
BA	r	s	t	u-v	w	x	y	z

Imaginons que l'on veuille transmettre le message « Venez » à un de nos amis. Le texte chiffré avec l'alphabet bilitère sera BAABB AABAA ABBAA AABAA BABBB.

Cette conversion est la première étape du procédé. Il faut ensuite un « texte de couverture » qui peut être absolument quelconque, mais cinq fois plus long que le message à transmettre. C'est un inconvénient de la méthode. Prenons par exemple comme texte de couverture la phrase « Il fait souvent froid en hiver ».

Ce texte sera imprimé avec deux types différents de caractères typographiques, que l'on peut appeler le type A et le type B. Ainsi, du texte apparent, on pourra déduire une séquence composée exclusivement de A et de B.

Dans notre exemple, le type A est représenté par les caractères romains, le type B par les italiques :

v					e					n					e					z				
B	A	A	B	B	A	A	B	A	A	A	B	B	A	A	A	A	B	A	A	B	A	B	B	B
I	l	f	a	i	t	s	o	u	v	e	n	t	f	r	o	i	d	e	n	h	i	v	e	r

Le message secret sera donc écrit ainsi :

*I*l f*ai*t s*o*uv*e**n**t* froi*d* en *h*i*ver*.

Déchiffrement

À partir du texte de couverture, il faut d'abord reconstituer la séquence de A et de B. Décomposée en groupes de cinq lettres, celle-ci permettra, en utilisant l'alphabet décrit dans notre tableau, de rétablir le texte secret. Il faut en fait reconstruire le tableau ci-dessus, en partant de la dernière ligne pour remonter à la première.

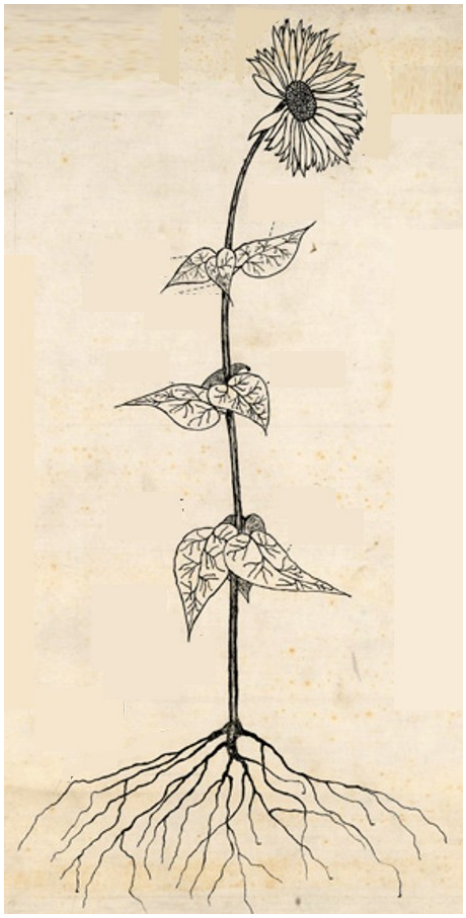
Le texte secret est entièrement indépendant du texte apparent. Bien entendu, la différence entre les deux types de caractères doit être très discrète, afin qu'elle échappe au lecteur non averti.

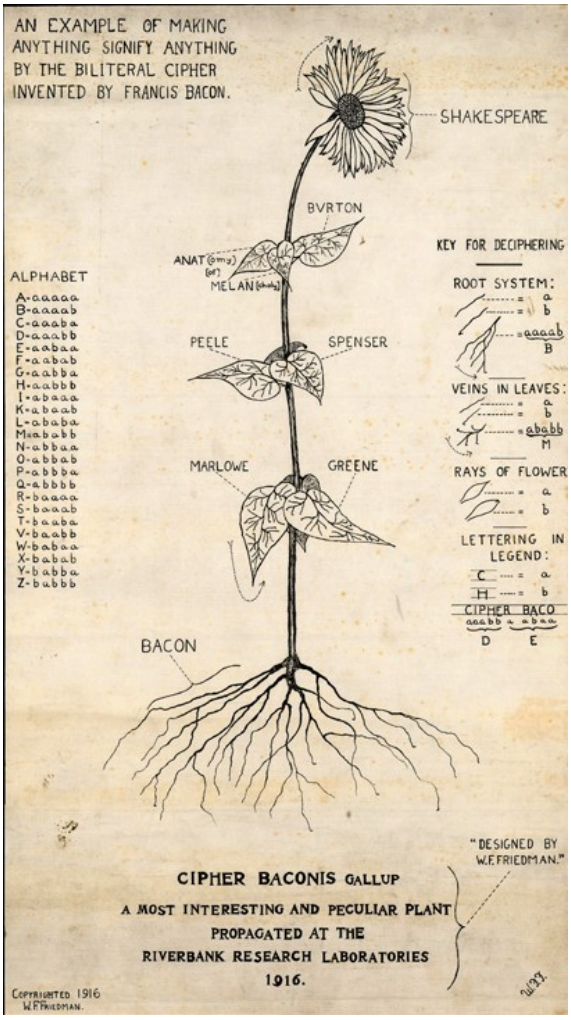
Le gros inconvénient de cette méthode est qu'elle est très fastidieuse et sujette aux erreurs aussi bien de chiffrement que de déchiffrement : il peut être délicat de reconnaître à quel groupe appartiennent les lettres.

Les messages cachés de William Friedman

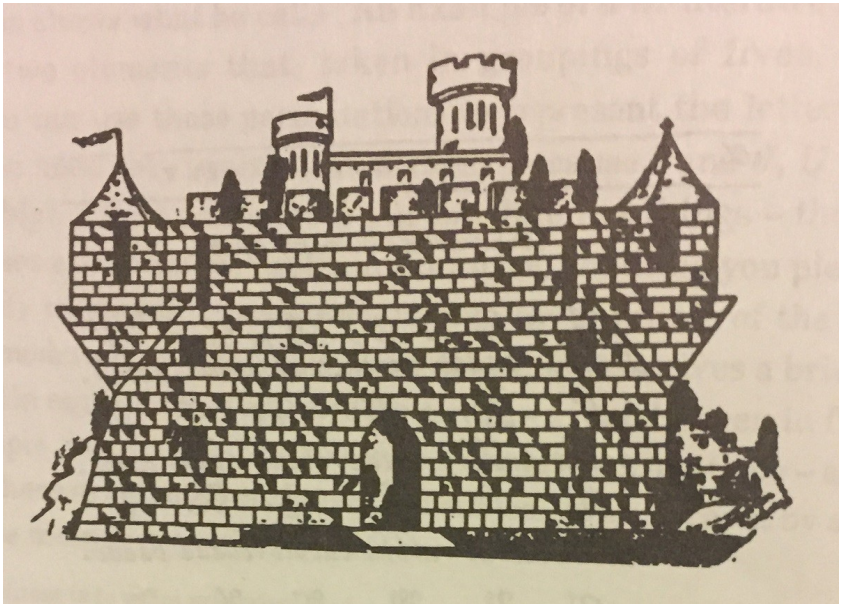
William Friedman aimait beaucoup le chiffre de Bacon, tellement qu'il a lui-même utilisé cet alphabet pour dissimuler des messages dans des dessins.

Voici le dessin d'un tournesol :





Soyons honnête, même en connaissant le secret, il est difficile de déchiffrer le message.
En voici un autre plus facile, qui utilise le même système de Bacon :



Ici, ce sont les briques du château qui dissimulent un message :

> *My business is to write prescriptions and then to see my doses staken*
> *but now I find I spend my time endeavoring to out-Bacon Bacon.*

Les Friedman sont indissociables du chiffre de Bacon, à tel point qu'Elizebeth a fait graver un message stéganographique sur leur pierre tombale, dans le cimetière d'Arlington. C'est la cryptologue américaine **Elonka Dunin**[4] qui a fait cette découverte en avril 2017 seulement.

Vous ne voyez pas ? Regardez attentivement l'épitaphe :

Cela ne saute pas aux yeux, mais si l'on regarde bien les E, on constate que les deux premiers sont écrits avec une police sans empattement, alors que le dernier est écrit avec empattement. Les lettres ont été écrites avec deux polices différentes ! Si l'on note par A une lettre sans empattement et B une lettre avec, on obtient :

```
KNOWL   EDGEI   SPOWE   R
BA?AA   AABAB   AA?AB   A  (difficile de dire si le O est avec ou sans empattement...)
```

En se référant à l'alphabet bilitère de Bacon, on déchiffre :

R ou W F B ou F : W. F. F. : William Frederick Friedman…

[4] http://elonka.com/friedman/index.html

Variantes : les chiffres trilitères

Le chiffre trilitère le plus connu est celui de **Friderici** donné dans son ouvrage *Cryptographia* publié en 1685. Mais, avant lui, d'autres cryptographes avaient reproduit des alphabets trilitères dans des manuels publiés en 1557 (**Cardan**), 1586 (**Vigenère**) et 1641 (**Wilkins**).

L'avantage par rapport aux chiffres bilitères est qu'on n'a besoin que de trois symboles pour définir une lettre au lieu de cinq.

Ces alphabets sont reproduits ci-dessous. Comme pour le chiffre bilitère de **Bacon**, le procédé de chiffrement repose sur l'alternance de trois types de caractères typographiques, qui sont notés ci-dessous A, B et C.

a	AAB	g	ACB	n	BAC	t	CAC
b	AAC	h	ACC	o	BCB	u-v	CAA
c	ABA	i-j	BBA	p	BCA	w	CAB
d	ABB	k	BBC	q	BCC	x	CBC
e	ABC	l	BAB	r	CCA	y	CBA
f	ACA	m	BAA	s	CCB	z	CBB

*Alphabet trilitère de **Friderici** (1685)*

a	AAC	g	ABC	n	CCB	t	BAC
b	AAB	h	CAC	o	CBA	u-v	BAB
c	ACA	i-j	ABB	p	CBC	w	BAB
d	ACC	k	CAB	q	CBB	x	BCA
e	ACB	l	CAA	r	BAA	y	BCC
f	ABA	m	CCA	s	CCC	z	BCB

*Alphabet trilitère de **Cardan** (1557)*

a	BBA	g	ACA	n	CCC	t	CBA
b	BAA	h	ACC	o	CCA	u-v	CBC
c	BAC	i-j	ACB	p	CCB	w	CBC
d	AAA	k	ABA	q	CAA	x	CBB
e	AAC	l	ABC	r	CAC	y	BBB
f	AAB	m	ABB	s	CAB	z	BCB

*Alphabet trilitère de **Vigenère** (1587)*

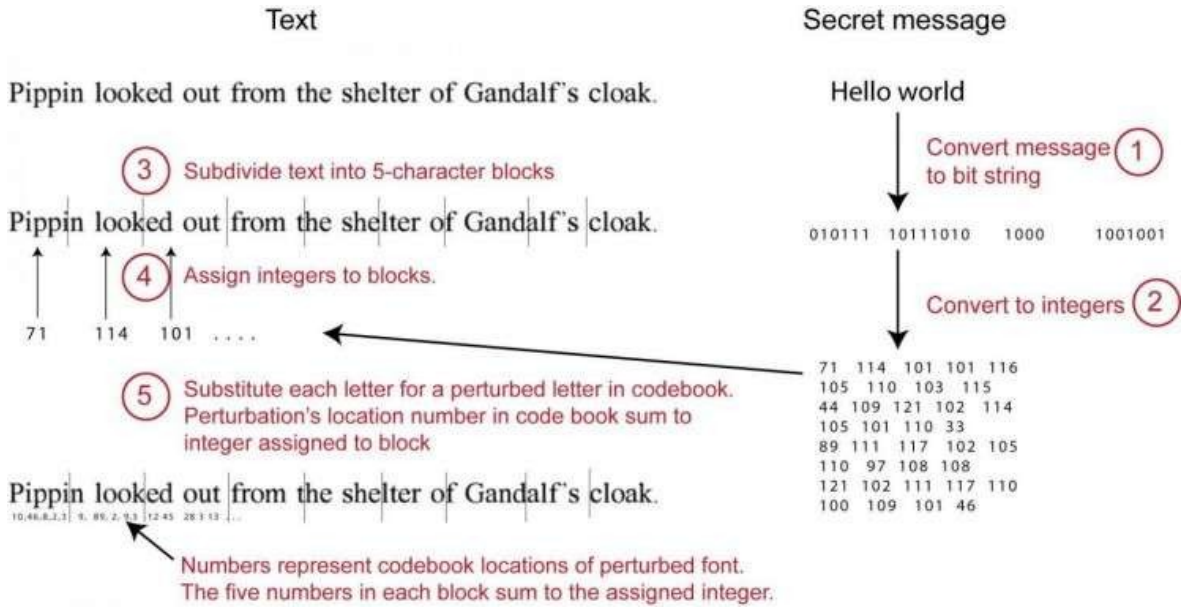
a	AAA	g	BBC	n	ABB	t	BCB
b	AAB	h	CAA	o	ABC	u-v	BCC
c	AAC	i-j	CCA	p	ACA	w	BAB
d	BAA	k	CCB	q	ACB	x	CBA
e	BBA	l	CCC	r	ACC	y	CBB
f	BBB	m	ABA	s	BCA	z	CBC

*Alphabet trilitère de **Wilkins** (1641)*

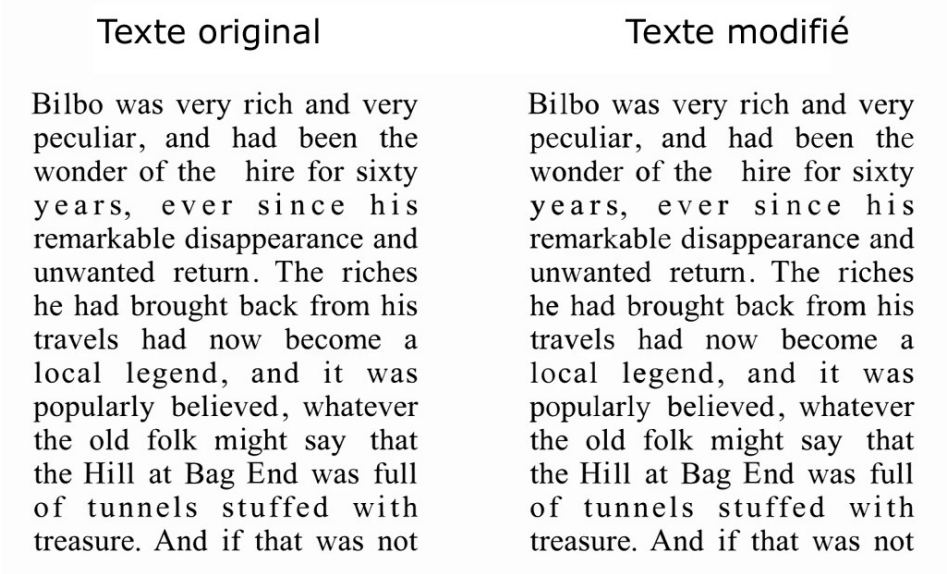
Une version moderne de l'idée de Francis Bacon

Le cryptage mis au point par **Changxi Zheng** et deux étudiants de l'université de Columbia (New York) est encore plus subtil, puisqu'il peut être utilisé avec n'importe quel texte, image ou fichier, et préserve le cryptage même lorsque le document est scanné, imprimé ou converti dans un autre format. Il est par exemple possible de photographier le texte avec un smartphone et de l'envoyer par texto à quelqu'un qui pourra y lire le message caché à l'aide du logiciel de décryptage.

Il repose sur une nouvelle police de caractères baptisée *FontCode*. Elle introduit des modifications de la forme des lettres imperceptibles à l'œil nu : largeur du trait, hauteur des lettres, atténuation des courbes des lettres rondes, etc. Le message à transmettre est d'abord converti en une suite de chiffres, chaque chiffre étant assigné à un bloc de cinq lettres dans un texte quelconque. Les lettres de ce texte sont ensuite modifiées par un algorithme qui choisit une altération. Pour décrypter le message encodé, l'algorithme identifie la place des lettres qui ont été altérées et en ressort le chiffre associé. « *L'information cachée, imperceptible pour l'œil humain, est lisible par une machine comme avec un lecteur de code-barres ou de QR code, sauf que sa présence est invisible* », explique **Changxi Zheng**.



© Changxi Zheng, Columbia Engineering



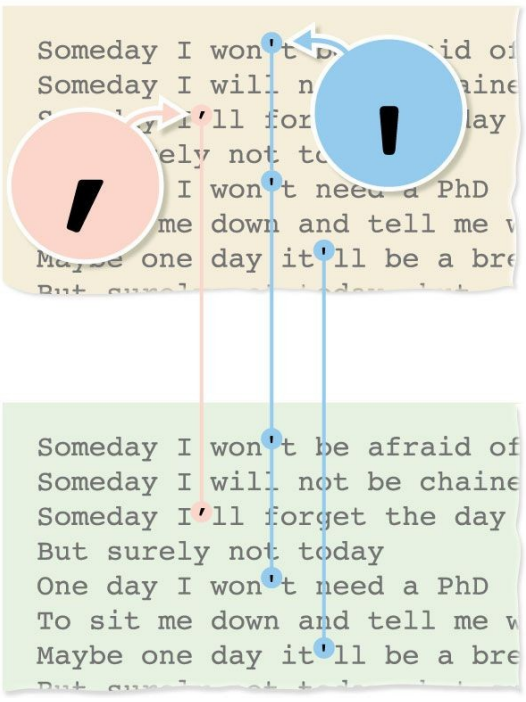
Les chercheurs envisagent de multiples applications possibles pour *FontCode* : QR codes invisibles sur des emballages ou des affiches, authentification de contrats ou d'actes légaux, protection contre la falsification de documents, etc.

Le lecteur qui veut en savoir plus trouvera son bonheur dans les références du § 2.14.

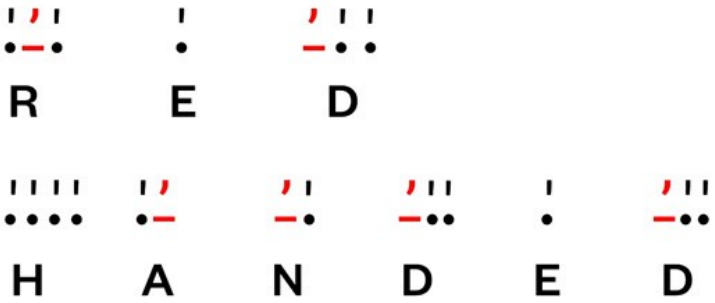
Comment Google s'est fait prendre « la main dans le sac »

Le 16 juin 2019, *The Wall Street Journal* a rapporté que *Genius*, le site Internet des paroles de chansons, avait déclaré avoir surpris Google en flagrant délit en train de voler les paroles de leur site Web sans aucune attribution ni aucun paiement. Google nie mais va enquêter sur la situation.

La façon dont Genius a attrapé Google était plutôt maligne. Deux formes d'apostrophes ont été utilisées dans les paroles :



Cette suite d'apostrophes signifie en Morse : « Red Handed » (l'équivalent de « la main dans le sac » en français) :



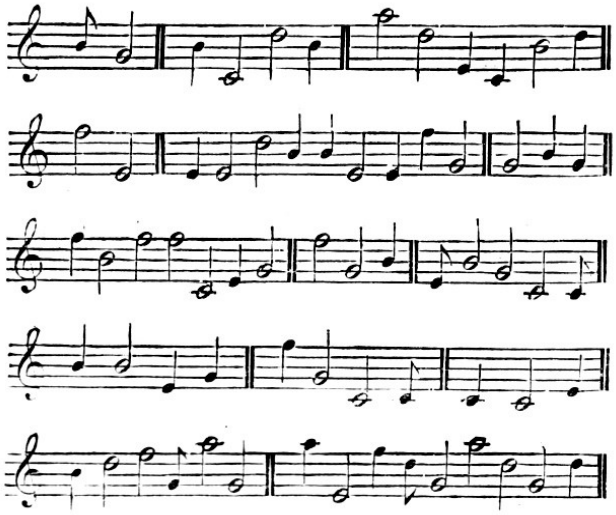
En comparant attentivement les paroles des deux sites, on voit que tout est absolument identiques, y compris les apostrophes. Cela prouve bien le copié-collé.

2.5. Sémagrammes

Le terme « sémagramme » vient du grec σημα (le signe), et γραμμα, (le texte écrit). Les éléments du texte codé ou chiffré ne sont ni des lettres, ni des chiffres : le sens est véhiculé par différents éléments, par exemple des points de jetons de dominos, l'emplacement d'objets sur une image, etc.

Selon **David Kahn**, le spécialiste mondial de l'histoire des codes secrets, le premier sémagramme connu est un procédé décrit par **Énée le Tacticien** (Én., *Poliorketica*, XXXI, 17-21), où un fil passe dans des trous percés dans un disque ou un osselet, chaque trou représentant une lettre.

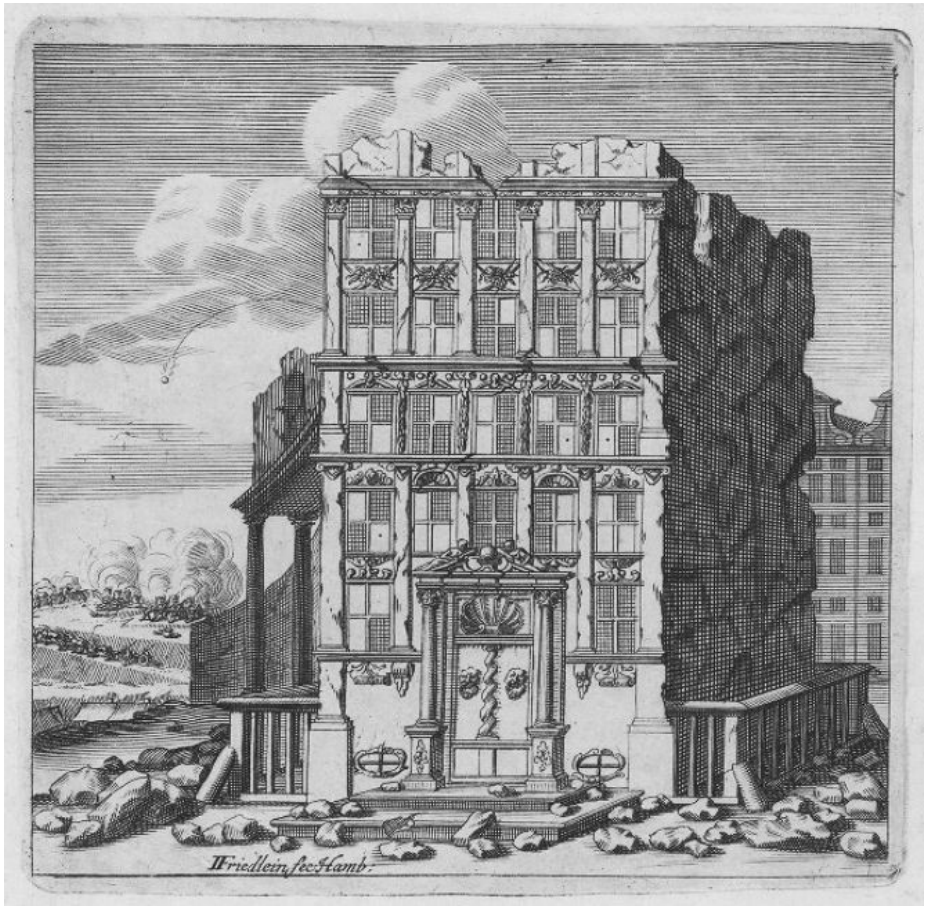
L'exemple suivant provient du livre de **Charles Joliet** *Les écritures secrètes dévoilées* [JOLI74]. Trois signes sont employés : la blanche, la noire et la croche. Leur position sur la portée détermine leur valeur alphabétique. Par exemple, le sol en note blanche est un « e ».

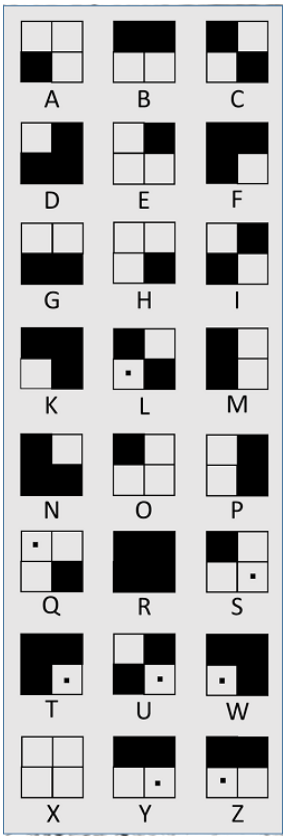


Le message caché est « Je suis Lindor, ma naissance est commune,
mes voeux sont ceux d'un simple bachelier. »

Gaspar Schott (1608–1666) présentait déjà ce procédé, consistant à remplacer une lettre par une note, dans son livre *Schola Steganographica* (1665). **Schott** a également étendu le code *Ave Maria* proposé par l'abbé **Trithème** (voir § 2.2). Le code étendu utilise 40 tables, chacune contenant 24 entrées (une pour chaque lettre de l'alphabet) dans quatre langues : latin, allemand, italien et français.

Dans son ouvrage *Cryptographia oder Geheime Schrifft-münd-und Würkliche Correspondentz* (1684/1685), **Johannes Balthasar Friderici** (1639 - env. 1704) nous montre un dessin apparemment anodin, mais qui contient un message secret. Ce message est codé par les fenêtres de l'immeuble : WIR HABEN KEIN PULVER MEHR (nous n'avons plus de poudre).





Alphabet chiffré

Des dessins d'enfants peuvent aussi cacher des messages :

Le même message est caché dans le dessin de Sybille, chaque lettre étant codée en Morse (voir § 5.5) avec une touffe d'herbe. Un petit brin signifie « point » et un long « trait ».

Dans le dessin d'Emlyn, ce sont les oiseaux qui codent le message « Je vous aime ». La lecture se fait du haut vers le bas. La position horizontale des oiseaux correspond à une lettre. Évidemment, on prendra soin d'envoyer séparément le dessin et la bande de lettres du haut de la page !

Cette idée figure déjà dans le livre de **Vigenère** *Traicté des chiffres, ou secretes manieres d'escrire* [VIGE86], où l'on voit le dessin d'un ciel nuageux avec des étoiles savamment disposées.

Saurez-vous trouver le message salace dissimulé dans ce billet de banque ?

Le 30 septembre 2010, Google célèbre les 50 ans des Pierrafeu avec un de ces célèbres Doodles.

Habilement dissimulé dans le dessin, on peut lire « Google » : le premier G est le véhicule, les 2 O les entrées des huttes, le second G le dinosaure, le L est le palmier, et on peut deviner un E formé par les fenêtres de la dernière hutte.

2.6. Micropoint

En 1857, **David Brewster** (1781–1868) suggérait de cacher des messages secrets dans un espace à peine plus grand qu'un point d'encre. En 1860, le problème de réduction des photographies était résolu par **René Dargon** (1819–1900).

C'est pendant la guerre franco-allemande de 1870-1871 que l'on vit les premiers usages militaires du microfilm. Des messages microfilmés étaient transportés par pigeons voyageurs. Durant la Seconde Guerre Mondiale, les agents allemands utilisaient la technique du micropoint de *Zapp*, qui consistait à réduire la photo d'une page en un point de moins d'un millimètre de diamètre. Il était ensuite apposé sous forme de point dans des magazines, dans une lettre anodine, parfois sous un timbre, etc.

Le procédé est évoqué dans l'aventure de Blake et Mortimer, *SOS météores*.

On trouve aussi une variante du micropoint sur tous les billets de banque suisses en circulation entre 1997 et 2017.

Voici un ancien billet de dix francs :

recto

verso

Portrait au recto
Le Corbusier, 1887–1965, architecte, urbaniste, peintre, théoricien

Motifs au verso
Palais de Justice de Chandigarh
Façade du secrétariat
Le Modulor
Bâtiment du secrétariat

Graphiste
Jörg Zintzmeyer

L'image ci-contre a été obtenue en agrandissant fortement le petit carré entouré d'un cercle noir au verso du billet : on a scanné cette partie du billet avec une résolution de 2400 ppi pour voir apparaître le texte (une simple loupe ne permet pas de lire les caractères).

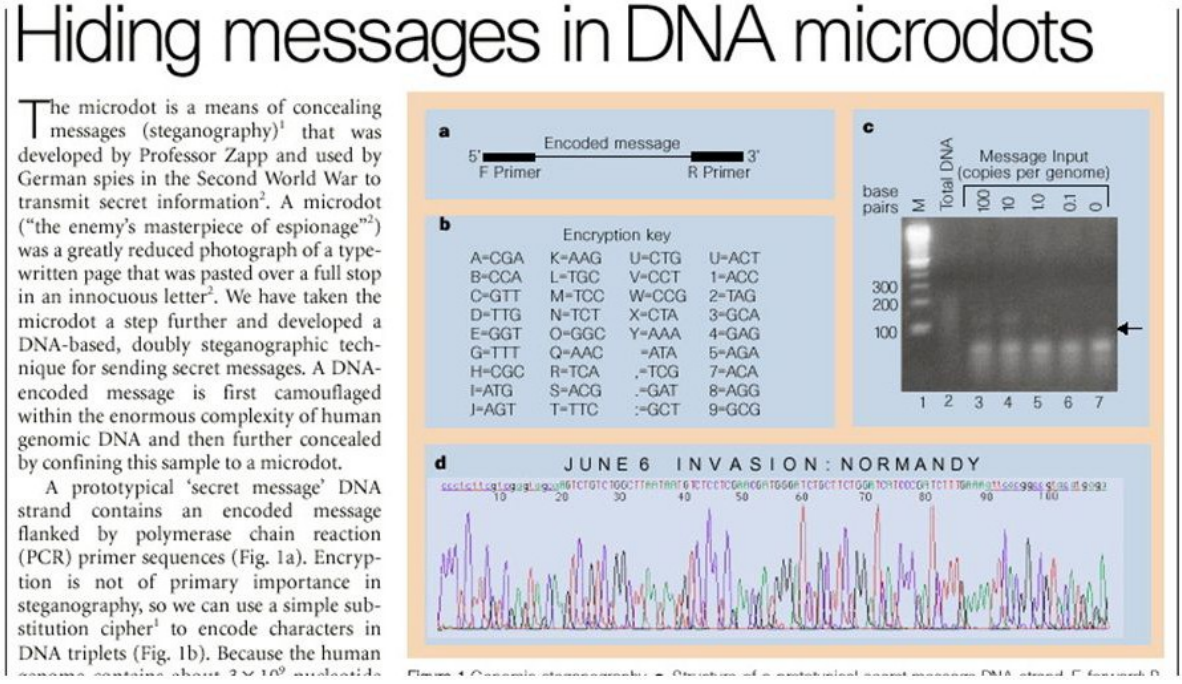
Les permis de conduire suisses possèdent aussi des micropoints. Regardez au-dessus du rond rouge, du triangle jaune et du carré vert. Il y a une ligne noire séparant la partie grise de la partie rose. Si vous prenez une loupe, vous lirez un texte où il est écrit « permis de conduire » dans toutes les langues, comme à l'avant du permis. Sauf qu'il y a une faute d'orthographe : il n'est pas écrit « permis de conduire » mais « permis de conduiere ».

Permis de conduire suisse

Agrandissement de la zone au-dessus des figures géométriques

Le permis de conduire suisse possède en effet plusieurs éléments de sécurité et l'introduction volontaire de certaines erreurs typographiques en fait partie… Cette technique de faire une erreur volontairement peut paraître simpliste, mais elle n'est pas nouvelle. Par exemple, les agents du *SOE* (voir § 4.10) faisaient volontairement une erreur à un endroit convenu du message afin de s'identifier : s'il n'y avait pas d'erreur, on pouvait penser que le message avait été envoyé par un agent ennemi.

En 1999, **Catherine Taylor Clelland, Viviana Risca** et **Carter Bancroft** publient dans la revue *Nature* leur article « Hiding messages in DNA microdots » (cacher des messages dans des micropoints d'ADN). Notre matériel génétique est en effet formé de l'enchaînement de quatre nucléotides que l'on peut comparer à un alphabet de quatre lettres : A, C, G et T. Or, les scientifiques sont maintenant capables de fabriquer des chaînes d'ADN avec une suite de nucléotides déterminée à l'avance. Il suffit alors d'attribuer un groupe de trois nucléotides à chaque lettre de l'alphabet, aux chiffres et aux signes de ponctuation (par exemple « A » = CGA, « B » = CCA, etc.) et de composer le « message génétique ». Pour brouiller les pistes, on peut ensuite le mélanger avec d'autres séquences aléatoires d'ADN. Le tout est à peine visible au microscope électronique. Comme application possible, on peut imaginer qu'une compagnie qui produirait une nouvelle espèce de tomate pourrait ainsi inclure sa marque de fabrique dans les molécules de la tomate, afin d'éviter les contrefaçons.



Hiding messages in DNA microdots

The microdot is a means of concealing messages (steganography)[1] that was developed by Professor Zapp and used by German spies in the Second World War to transmit secret information[2]. A microdot ("the enemy's masterpiece of espionage"[2]) was a greatly reduced photograph of a typewritten page that was pasted over a full stop in an innocuous letter[2]. We have taken the microdot a step further and developed a DNA-based, doubly steganographic technique for sending secret messages. A DNA-encoded message is first camouflaged within the enormous complexity of human genomic DNA and then further concealed by confining this sample to a microdot.

A prototypical 'secret message' DNA strand contains an encoded message flanked by polymerase chain reaction (PCR) primer sequences (Fig. 1a). Encryption is not of primary importance in steganography, so we can use a simple substitution cipher[1] to encode characters in DNA triplets (Fig. 1b). Because the human

Clelland et al., Nature 399:533 (1999). Hiding messages in DNA microdots

Une application évidente de la technique du micropoint est l'antisèche. Certains sites web[5] proposent de créer de fausses étiquettes de produits que l'on trouve couramment sur un banc d'élève : correcteur liquide (voir ci-contre), bâton de colle, bouteille d'eau, etc. L'idée toute simple est de remplacer les zones de texte que l'on ne lit jamais (composition, avertissement, etc.) par du texte utile pour tricher, écrit en très petit.

Évidemment, il faut avoir de bons yeux...

En novembre 2004, le magazine informatique *PC World* publiait un article[6] intitulé « Government Uses Color Laser Printer Technology to Track Documents » (« Le gouvernement[7] utilise la technologie des imprimantes laser couleur pour tracer les documents »). Selon cet article, « plusieurs sociétés d'imprimantes encodent discrètement le numéro de série et le code de fabrication de leurs imprimantes laser couleur et copieurs couleur sur tous les documents produits par ces machines. »

Le procédé décrit par *PC World* est le suivant : lorsqu'une imprimante couleur (ou une photocopieuse couleur) imprime un document, elle ajoute un motif de petits points jaunes (d'environ 0,1 millimètre de diamètre) au papier. Ces points, à peine visibles à l'œil nu, codent un message qui contient une identification de l'imprimante ainsi que la date et l'heure du processus d'impression. Ce procédé s'appelle le **MIC**, pour Machine Identification Code.

Ces points jaunes sur certaines imprimantes laser couleurs existent réellement depuis que **Xerox** l'a développé dans les années 1990. La raison principale des points jaunes était d'aider les services gouvernementaux dans les cas de contrefaçon de billets de banque.

On peut rendre les points visibles de différentes manières :

- numériser le papier avec une résolution d'au moins 600 DPI, et, avec un logiciel de traitement d'images, effectuer un agrandissement, puis modifier les couleurs et les contrastes pour que les points soient visibles ;
- dans une pièce sombre, illuminer le dos de la feuille avec une lumière ultraviolette et regarder avec une loupe. Les points jaunes sont maintenant noirs et plus visibles.

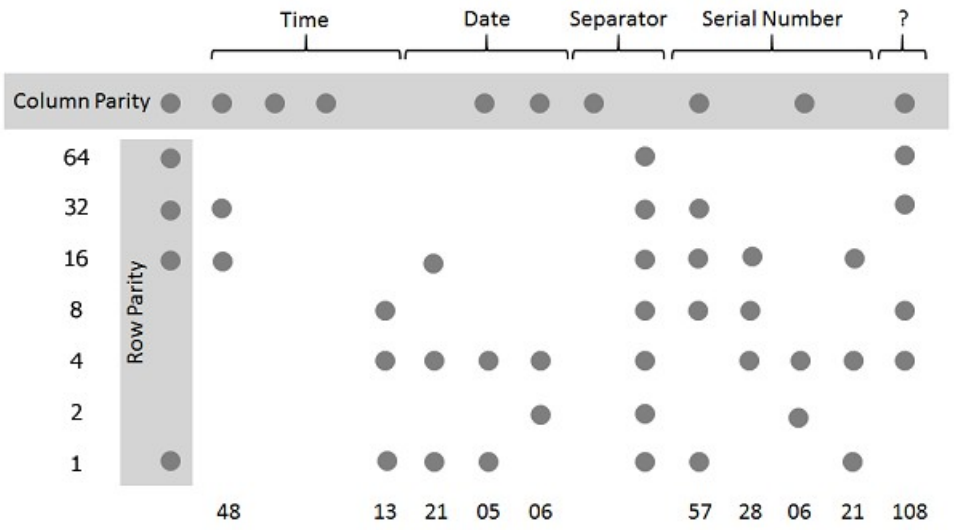
Dans les années qui ont suivi l'article de *PC World*, des membres de l'*Electronic Frontier Foundation* (*EFF*) ont examiné ces codes et ont découvert quelques détails à leur sujet. Cependant, ni un producteur d'imprimantes ni une autorité publique n'a jamais publié d'informations substantielles sur ce sujet.

Voici le code (non confirmé) utilisé par Xerox :

[5] Étant enseignant, il est clair que je ne vais pas donner l'adresse de ces sites !

[6] https://www.pcworld.com/article/118664/article.html

[7] américain



La colonne 10 était considérée comme un séparateur entre le numéro de série et la date et l'heure d'impression. Comme **Peter Buck** l'a découvert, c'est plutôt une ligne qui définit si un document a été imprimé ou copié. Si la colonne 10 est remplie, le document est imprimé. Si elle est vide, sauf le bit de parité, le document a été copié.

Peter Buck a écrit un papier de 30 pages intitulé *Printer Steganography, Reverse Ingineering the Machine Identification Code* en juin 2018.

2.7. Acrostiches

Un acrostiche est un poème dans lequel les initiales de chaque vers composent une phrase ou un mot.

Une tombe au cimetière Notre-Dame-des-Neiges de Montréal

La dernière strophe du *Dormeur du val* d'**Arthur Rimbaud** contient le mot *lit* :

Les parfums ne font pas frissonner sa narine;
Il dort dans le soleil, la main sur sa poitrine

Tranquille. Il a deux trous rouges au côté droit.

On trouve un autre exemple d'acrostiche aux vers 444 à 450 d'*Horace,* de **Corneille**. Est-il volontaire ? Difficile à dire. En tout cas, la probabilité que ce soit fortuit est très faible. On peut l'estimer grossièrement à 1 chance sur 3 millions, en comptant dans un dictionnaire le nombre de pages avec les mots commençant par S, A, L, E, C et U.

S'attacher au combat contre un autre soi-même,
Attaquer un parti qui prend pour défenseur
Le frère d'une femme et l'amant d'une sœur
Et rompant tous ces nœuds, s'armer pour la patrie
Contre un sang qu'on voudrait racheter de sa vie,
Une telle vertu n'appartenait qu'à nous;
L'éclat de son grand nom lui fait peu de jaloux...

Une étudiante de l'université Tufts, à Boston, aux États-Unis, a fait une découverte plutôt inattendue dans le poème épique *Paradise Lost* (*Le Paradis perdu* en version française) de **John Milton**, publié en 1667 puis en version complète et définitive, en 1674.

P. J. Klemp, professeur d'anglais à l'université de Wisconsin-Oshkosh, avait mis le doigt en 1977 sur un détail croustillant du poème épique. Dans le livre 9 de l'œuvre, vers 510 à 514, il avait repéré un acrostiche permettant de lire « SATAN », un des personnages principaux de ce poème décrivant la disparition la chute de l'homme du paradis, à travers le pêché d'Adam et Ève.

Scipio, the highth of Rome. With tract oblique
At first, as one who sought access, but feared
To interrupt, side-long he works his way.
As when a ship, by skilful steersman wrought
Nigh river's mouth or foreland, where the wind

Miranda Phaal, diplômée en 2018 de l'université Tufts, a découvert en 2019 un autre acrostiche, tout aussi saisissant, toujours dans le livre 9 du poème épique, cette fois, entre les vers 333 et 341.

From his surmise proved false; find peace within,
Favour from Heaven, our witness, from the event.
And what is faith, love, virtue, unassayed
Alone, without exteriour help sustained?
Let us not then suspect our happy state
Left so imperfect by the Maker wise,
As not secure to single or combined.
Frail is our happiness, if this be so,
And Eden were no Eden, thus exposed.

On peut lire à l'aide des premières lettres de ces quelques lignes trois fois (deux fois de haut en bas, puis une fois de bas en haut) le mot « FALL », soit la « chute », un mouvement central dans *Le Paradis perdu* de John Milton, puisque le poème décrit à la fois la chute de Lucifer (dans la première partie), puis celles d'Adam et Ève hors du Paradis...

Virgile a signé l'Énéide

Le célèbre poète romain **Virgile** aurait apposé sa signature en langage codé au début de son épopée, *L'Énéide*. Cette découverte datant de 2012 émane de **Cristiano Castelletti**, chercheur au domaine de philologie classique à l'Université de Fribourg (Suisse).

Voici les quatre premiers vers de l' *Énéide.*

Arma uirumque cano, Troiae qui primus ab ori**S**
Italiam fato profugus Lauiniaque ueni**T**
Litora - multum ille et terris iactatus et alt**O**
Vi superum, saeuae memorem Iunonis ob ira**M**

(Virgile, Énéide I, 1-4)

On a ici affaire à un acrostiche *boustrophédon*, qui consiste à alterner la direction de lecture : les vers impairs, on lira la première lettre puis la dernière du vers ; les vers pairs, on lira d'abord la dernière lettre puis la première. L'œil suit le même mouvement des bœufs qui tiraient la charrue pour creuser les sillons dans les champs. Le terme vient en effet du grec ancien βουστροφηδόν (*boustrophêdón*), de βοῦς (*boũs*) « bœuf » et στροφή (*strophḗ*) « action de tourner ».

Ainsi, l'acrostiche « a stilo M(aronis) V(ergili) » pourrait être traduit de la façon suivante : « à partir du stilus de Virgile Maron ». Le *stilus* est une tige en métal permettant d'écrire sur des tablettes de cire.

F*** YOU (again)

L'affaire a fait grand bruit aux États-Unis, fin octobre 2009. Le gouverneur de Californie **Arnold Schwarzenegger** a écrit un acrostiche à l'Assemblée de son État dans une lettre où il expliquait son veto à une loi visant à étendre les pouvoirs financiers du port de San Francisco.

To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many unnecessary bills come to me for consideration. Water reform, prison reform, and health care are major issues my Administration has brought to the table, but the Legislature just kicks the can down the alley.

Yet another legislative year has come and gone without the major reforms Californians overwhelmingly deserve. In light of this, and after careful consideration, I believe it is unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger

Interrogé, le porte-parole du gouverneur de Californie, **Aaron McLear**, prétendit qu'il s'agissait d'une malheureuse coïncidence…

Il semble que cet exercice de style soit devenu populaire aux Etats-Unis. En effet, **Daniel Kammen** s'y est adonné dans sa lettre de démission au président des États-Unis. Cet envoyé spécial du département d'État pour la science a préféré partir de son poste de conseiller climatique auprès du gouvernement à cause des propos tenus par **Donald Trump** après les événements de Charlottesville en 2017. Il lui a donc envoyé une lettre annonçant son départ, avec une petite surprise cachée à l'intérieur.

Dans un post Twitter, publié mercredi 23 août 2017, le conseiller a rendu cette lettre publique. Il y explique notamment que « son échec à condamner les suprémacistes blancs et les néo-nazis », ainsi que ses remarques sur les violences raciales en Virginie, avaient attaqué « les valeurs fondamentales des États-Unis » et que cela a des « ramifications nationales et internationales ».

Si on lit la première lettre de chaque paragraphe, on peut lire I.M.P.E.A.C.H. pour *Impeachment*, la procédure de mise en accusation permettant au pouvoir législatif de destituer un haut fonctionnaire du gouvernement !

James May viré

James May, présentateur de l'émission *Top Gear* de la BBC, a été viré du magazine *Autocar* pour avoir caché un message dans l'*édition* de 1992 du *Road Test Yearbook Edition*. (couverture en bas à droite de l'image ci-dessous).

En effet, si l'on prend la lettrine rouge de chaque test de voiture, on obtient :

Je laisse le lecteur traduire...

2.8. Code de Trevanion

En 1648, **Sir John Trevanion**, partisan de **Charles 1er**, fut arrêté par les hommes de **Cromwell** et retenu au château de Colchester, dans l'Essex. Il attendait son exécution quand il reçut une lettre d'un ami, dont on peut supposer qu'elle a été examinée minutieusement par les gardiens. Cette lettre de réconfort d'apparence anodine renfermait un message d'une importance capitale pour lui.

Worthie Sir John : — Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honor, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command. - R.T.

Preux Sir John : — L'espoir, qui est le meilleur soutien des êtres dans l'affliction, ne peut plus guère, je le crains, vous être d'un grand secours à présent. Il est une chose cependant que j'aimerais vous dire : s'il existait jamais la possibilité de m'acquitter envers vous de tout ce dont je vous suis redevable, n'hésitez pas à faire appel à moi. Je ne puis faire grand-chose, mais soyez bien certain que je ferai tout ce qui est en mon pouvoir. Si l'heure de votre mort vient à sonner je sais que, contrairement aux autres hommes, vous l'envisagerez sans effroi et l'accueillerez comme un honneur rendu à votre loyauté. Priez à présent que cette coupe amère s'éloigne de vos lèvres. Je sais parfaitement bien que vous ne craignez nullement les souffrances, mais si elles peuvent vous être épargnées par une attitude soumise, ce serait faire acte de sagesse. Dites-moi s'il est une chose que je puisse faire pour vous, et je le ferai. Le général revient mercredi. Je suis, toujours à vos ordres, votre fidèle serviteur. — R.T.

En ne gardant que les troisièmes lettres après une ponctuation, on peut lire (dans la lettre originale en anglais, évidemment) : « Panel at east end of chapel slides » (le panneau à l'extrémité Est de la chapelle coulisse). Grâce à cette information, Sir John put s'échapper.

2.9. Lettres à double entente

Lettre de Richelieu à l'ambassadeur de France à Rome

M. Compigne, Savoyard de naissance, frère de l'ordre de Saint-Benoît,
est la personne qui vous présentera cette lettre comme un passe-port pour arriver à votre protection ;
C'est l'homme le plus discret, le plus sage et le moins
médiocre que je connaisse, et avec qui j'ai eu le plaisir de converser ;
il m'a longtemps sollicité de vous écrire en sa faveur, et
de lui délivrer un certificat convenable ainsi qu'une lettre de crédit,
ce que j'ai enfin accordé à son mérite réel plutôt qu'à son
importunité, car, croyez-moi, Mr, sa modestie n'est surpassée que par son mérite ;
je serais fâché que vous fussiez dans le cas de négliger de lui rendre service, faute
de méconnaître son caractère réel, je serais fâché que vous fussiez
comme l'ont été quelques-uns de ses amis intimes, induit dans une erreur qu'ils reconnaissent.
Je crois de mon devoir de vous prévenir que vous me ferez un sensible plaisir
de porter une attention particulière à tout ce qu'il fera, et de lui témoigner tout le respect possible,
et de ne pas vous hasarder à rien dire en sa présence qui puisse l'offenser ou lui déplaire
en aucune manière ; je puis vous dire qu'il n'y a personne que j'aime autant que M. Compigne,
personne que je regrettasse plus de voir négligé, parce qu'il n'y a personne plus digne d'être
reçu et admis dans la bonne société, il serait donc odieux de lui manquer
et je suis persuadé qu'aussitôt que vous connaîtrez ses vertus et que vous
l'apprécierez tel qu'il est réellement, vous l'estimerez comme je fais, et alors
vous me remercierez de mon avis ; la confiance que je mets dans
votre obligeance me force à m'abstenir de m'étendre davantage sur cette matière, ou
de rien dire de plus à ce sujet. Croyez-moi, Mr, etc.

RICHELIEU

Il ne faut lire que la moitié gauche de la lettre pour comprendre ce que **Richelieu** pensait vraiment de **M. Compigne…**

Correspondance entre George Sand et Alfred de Musset

Ces lettres codées, les plus connues de la langue française, n'ont en réalité été écrites ni par **George Sand**, ni par **Alfred de Musset**. Il s'agit d'un canular dont on évalue l'origine entre 1870 et 1915.

Lettre de George Sand à Alfred de Musset

Cher ami,

Je suis tout émue de vous dire que j'ai bien compris l'autre jour que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler, sans artifice, mon âme toute nue, daignez me faire visite, nous causerons et en amis franchement je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde, comme la plus étroite amitié, en un mot : la meilleure épouse dont vous puissiez rêver. Puisque votre âme est libre, pensez que l'abandon où je vis est bien long, bien dur et souvent bien insupportable. Mon chagrin est trop gros. Accourez bien vite et venez me le faire oublier. À vous je veux me soumettre entièrement.

Votre poupée

La correspondance continuait ainsi :

Quand je mets à vos pieds un éternel hommage,
Voulez-vous qu'un instant je change de visage ?
Vous avez capturé les sentiments d'un cœur
Que pour vous adorer forma le créateur.
Je vous chéris, amour, et ma plume en délire
Couche sur le papier ce que je n'ose dire.
Avec soin de mes vers lisez les premiers mots,
Vous saurez quel remède apporter à mes maux.

Alfred de Musset

Et George Sand répondit :

Cette insigne faveur que votre cœur réclame
Nuit à ma renommée et répugne à mon âme.

George Sand

Pour lire le vrai message contenu dans la première lettre, lisez une ligne sur deux. Quant aux deux autres lettres, il faut lire le premier mot de chaque phrase.

2.10. Stéganographie oulipienne

Fondé en 1960 par **Raymond Queneau** et **François Le Lionnais**, l'Oulipo (OUvroir de LIttérature POtentielle) se veut une tentative d'exploration méthodique des potentialités de la littérature, et plus généralement de la langue. Unissant à l'origine écrivains, mathématiciens, poètes et logiciens, ce projet vise à assembler les lettres et les mots selon des structures, des formes, des contraintes nouvelles, afin de produire des œuvres originales. Ainsi, **Georges Perec** a écrit un roman entier sans utiliser la voyelle *e* (*La disparition*) et un autre où la seule voyelle autorisée était le *e* (*Les revenentes*).

La belle absente

Champ défait jusqu'à la ligne brève,
J'ai désiré vingt-cinq flèches de plomb
Jusqu'au front borné de ma page chétive.

Je ne demande qu'au hasard cette fable en prose vague,
Vestige du charme déjà bien flou qui
défit ce champ jusqu'à la ligne brève.

Georges Perec, *A l'OuLiPo*

Les familiers des ouvrages oulipiens auront reconnu une « belle absente ». C'est un poème écrit à l'aide d'un alphabet simplifié (on supprime K, W, X, Y et Z). Dans chaque vers doivent apparaître, au moins une fois, toutes les lettres de cet alphabet sauf une : en lisant de haut en bas ces lettres manquantes, on verra apparaître le mot caché : OULIPO

Le domaine d'Ana

Dans son crypto-roman *Le domaine d'Ana*, **Jean Lahougue** a imaginé un système de dérivations multiples qui permet d'obtenir d'autres textes à partir du livre entier ou de certaines de ses sections. Ces dérivations s'effectuent grâce à un ensemble de règles que dévoile le cahier des charges du roman et dont voici les premières[8] :

- La lecture, dans l'ordre, des lettres centrales (*médiales*) des mots (ayant un nombre impair de lettres) du huitième chapitre du roman permettra la reconstitution d'un nouveau texte que nous appellerons le chapitre 8'.
- Le chapitre 8' obéira à la même règle des médiales. Celle-ci permettra la reconstitution d'un nouveau sous-texte dérivé que nous appellerons chapitre 8".
- Le chapitre 8" obéira à la même règle des médiales que les chapitres 8 et 8'. Le texte dérivé se réduira au mot : Ana.
- La lecture dans l'ordre inverse (en partant de la dernière phrase du dernier chapitre et en remontant jusqu'à la première du chapitre initial) des mots centraux (médiaux) de toutes les phrases du roman permettra la reconstitution d'un nouveau texte que nous appellerons roman'.
- La lecture, dans l'ordre, des médiales du roman' permettra la reconstitution d'un nouveau texte que nous appellerons roman".
- La lecture, dans l'ordre, des médiales du roman" permettra la reconstitution d'un nouveau texte que nous appellerons roman'".
- La lecture des médiales du roman'" permettra la reconstitution d'un nouveau texte se limitant au mot : Ana.

2.11. La méthode de Grandpré

Voici une méthode très raffinée, mêlant stéganographie et substitution homophone (voir chapitre 6), que **A. de Grandpré** propose dans son livre *Cryptographie pratique* [GRAN05]. L'idée est de cacher un texte dans une lettre anodine, de telle manière que personne, sauf le destinataire, ne sache qu'elle contient un message secret. De plus, pas besoin de livre de codes, mais seulement d'un peu de mémoire.

On commence par construire un tableau de dix lignes contenant des mots de dix lettres (on en trouvera facilement dans un dictionnaire de mots-croisés). Il faut que toutes les lettres de l'alphabet soient représentées dans ce tableau. Il suffira de se rappeler ces dix mots dans l'ordre pour reformer le tableau.

Chaque lettre de ce tableau sera repérée par ses coordonnées (numéro de la ligne, puis numéro de la colonne). On dira que 10 = 0, 11 = 1, etc. Par exemple, « t » = 16 ou 93. Il peut y avoir plusieurs possibilités pour la même lettre.

Il faut maintenant cacher un message dans une missive. Chaque lettre du message secret sera codée par deux mots dont le nombre de lettres sera, pour le premier, le numéro de la ligne, et, pour le second, le

[8] « Clés du domaine », dans **Ecriverons et liserons en vingt lettres**, de Jean-Marie Laclavetine et Jean Lahougue

numéro de la colonne. Ces mots seront espacés de quatre en quatre. Il faudra donc en tout huit mots pour représenter une lettre, dont six seront là seulement pour faire des phrases cohérentes et banales. Les mots séparés par une apostrophe ou un trait d'union comptent pour deux (par exemple « qu'il », « peut-être »).

Exemple

Tout cela semble bien compliqué. Voyons cela sur un exemple. Construisons d'abord le tableau avec les 10 mots de 10 lettres suivants : HYPNOTIQUE, DEVELOPPER, ANARCHISME, INJONCTION, KILOGRAMME, OMBILICAUX, RAFFINERIE, ZINZINULER, WATERPROOF et RAPSODISTE.

	1	2	3	4	5	6	7	8	9	0
1	h	y	p	n	o	t	i	q	u	e
2	d	e	v	e	l	o	p	p	e	r
3	a	n	a	r	c	h	i	s	m	e
4	i	n	j	o	n	c	t	i	o	n
5	k	i	l	o	g	r	a	m	m	e
6	o	m	b	i	l	i	c	a	u	x
7	r	a	f	f	i	n	e	r	i	e
8	z	i	n	z	i	n	u	l	e	r
9	w	a	t	e	r	p	r	o	o	f
0	r	a	p	s	o	d	i	s	t	e

Alice veut transmettre le message « je t'aime » à Bob. Mais sa femme a des soupçons, et il est très probable qu'elle lira le courrier de son mari.

En chiffres, le message sera codé par la suite 43-94-16-72-64-62-70. Il lui faudra donc écrire une lettre de 56 à 59 mots (les mots qui chiffrent le message sont soulignés).

> Cher Bob,
> Cela **fait** maintenant bientôt trois **ans** que notre magnifique **rencontre** a eu lieu, **dans** ce pays que j'aime tellement : la **Suisse**. Je souhaiterais vous **inviter** pour bien fêter **ce** bel anniversaire. Que **diriez**-vous si je **vous** conviais chez moi **samedi** ? Bien sûr que **je** serais ravie que **Sabrina**, votre épouse, vous **accompagne**.
>
> Cordialement,
>
> Alice

Pour la correspondance privée, ce chiffre est absolument indécelable et incassable, à moins de laisser traîner sur son bureau le tableau des dix mots ! Il est idéal pour les petits messages, mais inutilisable pour chiffrer rapidement de longs textes.

2.12. Le Barn code du SOE

Le *SOE* britannique (*Special Operations Executive*) dissimulait un court message dans une lettre ordinaire selon le **Barn Code**. Supposons qu'un agent reçoive par la poste la lettre ci-après :

Mon cher Pierre,
J'espère que tu voudras bien m'excuser, mais j'ai eu tellement de travail à la maison que je n'ai pas pris le temps d'écrire aux amis. Cependant je t'envoie ce petit mot d'urgence pour te faire savoir que si tu veux des pneus, tu ferais bien de te dépêcher; en effet :
Hier, Jean est venu nous rendre visite, il descendait du train et s'est arrêté un moment chez nous pour bavarder et donner des nouvelles à mon père de son Paris. En principe, il doit rester quelques jours ici pour mettre en ordre ses affaires avant de repartir pour la capitale. A Paris, c'est calme, mais la veille il avait été dérangé en plein sommeil par les sirènes deux fois dans la nuit! Ceci mis à part, il doit nous faire envoyer par un ami à lui des pneus neufs pour nos vélos. Il en a pour le moment, profitons-en! A bientôt de tes nouvelles.

P.-S. Nous irons au mariage de Simone et Henri, dimanche en quinze. Henri est un garçon sympathique qui a connu Simone l'an dernier chez Xavier, notre vieil ami. Il a deux ans de plus qu'elle et nous pensons que Simone va être très heureuse.

Cette lettre n'a aucune raison d'attirer l'attention. C'est pourtant un exemple sophistiqué de chiffrement qui combine deux techniques cryptographique : la stéganographie et la substitution selon le système de Playfair.

Extrayons le dixième mot du premier paragraphe : « Tellement » et disposons-le en haut d'un tableau. Écrivons sous chaque lettre son classement dans l'alphabet : la première lettre qui apparaît dans l'alphabet est le E. Comme il y en a trois, ils auront les numéros 1, 2 et 3. La suivante est le L. Il y en a 2 ; ils auront les numéros 4 et 5. Et ainsi de suite.

Écrivons ensuite le second paragraphe de la lettre sous cette clef.

T	E	L	L	E	M	E	N	T
8	1	4	5	2	6	3	7	9
Hier,	**Jean**	est	venu	nous	rendre	visite,	il	descendait
du	train	et	s'est	**arrêté**	un	moment	chez	nous
pour	bavarder	et	donner	des	nouvelles	**à**	mon	père
de	son	**Paris**.	En	principe,	il	doit	rester	quelques
jours	ici	pour	**mettre**	en	ordre	ses	affaires	avant
de	repartir	pour	la	capitale.	**A**	Paris,	c'est	calme,
mais	la	veille	il	avait	été	dérangé	**en**	plein
sommeil	par	les	sirènes	deux	fois	dans	la	nuit!
Ceci	mis	à	part,	il	doit	nous	faire	**envoyer**
par	**un**	ami	à	lui	des	pneus	neufs	pour
nos	vélos.	Il	en	**a**	pour	le	moment	profitons-
en!	A	bientôt	de	tes	nouvelles.			

Le texte clair apparaît quand on lit le tableau ligne par ligne, un mot par ligne, sous les colonnes repérées dans l'ordre numérique de la clef :

Jean arrêté à Paris. Mettre *a* en sommeil. Envoyer un *a*.

Il est convenu que les mots trop révélateurs sont indiqués par la lettre « *a* » et chiffrés par système de **Playfair** dans le post-scriptum. Par convention, le code commence avec la première lettre du quatrième mot, puis on saute chaque fois trois mots.

*Nous irons au **mariage** de Simone et **Henri**, dimanche en quinze. **Henri** est un garçon **sympathique** qui a connu **Simone** l'an dernier chez **Xavier**, notre vieil ami. **Il** a deux ans **de** plus qu'elle et **nous** pensons que Simone **va** être très heureuse.*

Les lettres sont : **M**ariage, **H**enri, **H**enri, **S**ympathique, **S**imone, **X**avier, **I**l, **D**e, **N**ous, **V**a.

Le texte chiffré à déchiffrer est : MH HS SX ID NV. S'il avait été entendu, au préalable, que la grille du Playfair serait formée avec les mots « Shakespeare and Milton », nous aurions (voir § 9.2) :

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

Texte chiffré : MH HS SX ID NV

Texte clair : RE SE AU OP RX

D'où le texte complètement déchiffré :
« Jean arrêté à Paris. Mettre réseau en sommeil. Envoyer un OPR (opérateur radio). »

2.13. Message caché dans une image numérique

Depuis l'avènement des ordinateurs, un des exemples les plus étonnants de stéganographie est la possibilité de cacher une image numérique dans une autre.

Sur un écran, une image est constituée de pixels. La couleur de chaque pixel est un mélange de rouge (R), de vert (G pour green), et de bleu B. C'est le système RGB. L'intensité de rouge, de vert, de bleu de chaque pixel est un nombre compris entre 0 et 255.

Chacun de ces nombres s'écrit en base 2 comme une suite de 8 bits (0 ou 1). Cela forme un octet. 00000000 = 0 ; 00000001 = 2^0 = 1 ; 00000010 = 2^1 = 2 ; 10000011 = $2^7 + 2^1 + 2^0$ = 131 ; 11111111 = $2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$ = 255.

Parenthèse mathématique

En base dix, on a besoin de dix chiffres, de 0 à 9 ; en base *n*, on a besoin de *n* chiffres ou symboles, de 0 à *n*–1 ; en base deux, on a besoin de deux chiffres : 0 et 1.
Un nombre qui s'exprime en base B par les quatre chiffres 1011 s'analyse :

en base *B* : $1xB^3 + 1xB^2 + 0xB^1 + 1xB^0$
en base 10 : $1x10^3 + 1x10^2 + 0x10^1 + 1x10^0 = 1011$
en base 8 : $1x8^3 + 1x8^2 + 0x8^1 + 1x8^0 = 577$
en base 2 : $1x2^3 + 1x2^2 + 0x2^1 + 1x2^0 = 13$

La technique de base, dite *LSB* pour *least significant bit*, consiste à modifier les bits de poids faible des pixels codant l'image. Prenons l'octet 10010011 (en base 10, $2^7 + 2^4 + 2^1 + 2^0$ = 147). Si l'on remplace les 4 bits de poids faibles (ceux de droite) par 1110, on obtiendra l'octet 10011110 (en base 10, $2^7 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$ = 158). La différence de couleur sera trop faible à pour être perceptible à l'oeil nu.

Prenons un pixel d'une image A, et le même pixel d'une image B. Ces deux pixels sont chacun caractérisés par 3 octets. On va fabriquer un seul pixel qui sera presque colorié comme celui provenant de l'image A. C'est donc l'image A qui va dissimuler l'image B. Pour cela, on garde les 4 premiers bits de

chaque couleur du pixel de l'image A, et on complète l'octet par les 4 premiers bits de chaque couleur du pixel de l'image B, comme dans l'exemple ci-dessous.

	Rouge (V)	Vert (G)	Bleu (B)
Pixel de l'image A	**1001**0011	**1110**0011	**1010**1111
Pixel de l'image B	11111100	01101110	11010101
Pixel de l'image C	**1001**1111	**1110**0110	**1010**1101

L'image que l'on aura ainsi fabriquée sera très proche de la première image. Pour chaque pixel, on a changé l'intensité de rouge, de vert et de bleu d'au plus 16 (sur une valeur comprise entre 0 et 255).

Voyons maintenant comment, à partir de l'image C, retrouver les images A et B. Pour chaque pixel de l'image C, on regarde les quatre premiers bits de l'intensité de rouge, de vert et de bleu. Ces quatre premiers bits vont constituer les quatre premiers bits de rouge, vert et bleu du pixel correspondant de l'image A'. On complète chaque octet par quatre zéros. Les quatre derniers bits de l'intensité de rouge, vert, bleu de chaque pixel de l'image C vont eux constituer les quatre premiers bits de l'image B'. On complète là aussi chaque octet par quatre zéros.

	Rouge (V)	Vert (G)	Bleu (B)
Pixel de l'image C	**1001**1111	**1110**0110	**1010**1101
Pixel de l'image A'	**1001**0000	**1110**0000	**1010**0000
Pixel de l'image B'	11110000	01100000	11010000

Comme on le voit, on ne retrouve pas exactement les images de départ, mais elles sont absolument reconnaissables.

On peut aussi cacher un texte dans une image numérique et cela de manière parfaitement invisible à l'œil nu. Cette technique s'appelle le tatouage (*watermarking* en anglais). Elle est utilisée notamment pour protéger des images par copyright, mais on peut évidemment aussi transmettre des messages cachés. Je vais montrer ici une méthode simple, mais qui fonctionne seulement avec certains formats d'images, notamment le format TIFF. En effet, beaucoup de formats compressent les données et donc modifient les bits de l'image, ce qui a pour effet de détruire le message caché. On avait d'ailleurs le même problème en dissimulant une image dans une autre image…

Représentation binaire du texte

La mémoire de l'ordinateur conserve toutes les données sous forme binaire. Il n'existe pas de méthode pour stocker directement les caractères. Chaque caractère possède donc son équivalent en code numérique : c'est le **code ASCII** (*American Standard Code for Information Interchange*).

Le code ASCII a été mis au point pour la langue anglaise, il ne contient donc pas de caractères accentués, ni de caractères spécifiques à une langue. Le code ASCII a donc été étendu à 8 bits (un octet) pour pouvoir coder plus de caractères (on parle d'ailleurs de code ASCII étendu...). Ce code attribue les valeurs 0 à 255 aux lettres majuscules et minuscules, aux chiffres, aux marques de ponctuation et aux autres symboles (caractères accentués dans le cas du code *iso-latin1*).

Le code ASCII de base représentait les caractères sur 7 bits (c'est-à-dire 128 caractères possibles, de 0 à 127).

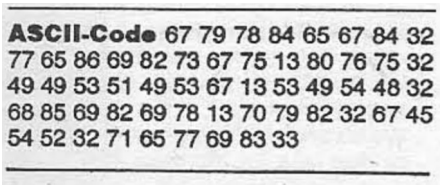
- Les codes 0 à 31 ne sont pas des caractères. On les appelle *caractères de contrôle*.
- Les codes 65 à 90 représentent les majuscules.
- Les codes 97 à 122 représentent les minuscules.

code	0	1	2	3	4	5	6	7	8	9
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT
10	LF	VT	NP	CR	SO	SI	DLE	DC1	DC2	DC3
20	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS
30	RS	US	SP	!	"	#	$	%	&	'
40	(	)	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~	DEL		

Code ASCII

Chaque caractère du texte à cacher sera représenté par son code ASCII étendu, écrit en base 2. Par exemple, le code ASCII de « A » est 65, ce qui donne en binaire, sur un octet : 01000001. Le texte complet sera donc une suite de 0 et de 1, chaque caractère utilisant 8 bits.

Juste en passant, voici une petite annonce publiée dans le magazine informatique *ASM* dans les années 1980 :



C'est un encodage utilisant le code ASCII. En décodant le message avec le tableau ci-dessus, on obtient :

CONTACTEZ MAVERICK PLK 115315 C 5160 DUEREN POUR LES JEUX C-64!

Düren (ancien code postal : 5160) est une ville d'Allemagne, près de Cologne. *PLK* signifie *Postlagerkarte*. C'était un service postal allemand qui permettait aux clients de recevoir du courrier de manière anonyme, sans fournir de documents d'identification. Il a été introduit par la poste impériale allemande en 1910 et aboli en 1991. Le numéro 115315 C était l'identification PLK de la personne qui a placé l'annonce.
Apparemment, le but de cette publicité était de vendre des copies piratées de jeux pour Commodore 64, un des ordinateurs personnels mythiques de l'époque. Comme c'était illégal, l'industrie du logiciel a forcé les magazines informatiques à cesser de publier des publicités avec un tel contenu. En cryptant leurs messages, les vendeurs de logiciels illégaux ont tenté de contourner cette censure. Cette astuce a fonctionné pendant un certain temps, avant que les magazines informatiques ne finissent par rejeter les publicités illégales, même si elles n'étaient pas immédiatement lisibles.

Intégration du texte dans l'image

Si on travaille en base 10, on peut imaginer l'image comme une suite de nombres compris entre 0 et 255. La technique de camouflage que je propose ici reprend l'idée du chiffre bilitère de **Francis Bacon** (§ 2.4) : on va dire qu'un nombre pair correspond à un 0 du texte et qu'un nombre impair correspond à un 1. Il faudra donc modifier certains pixels de l'image, mais ces altérations seront invisibles.

Si le nombre du tableau de l'image a la parité que l'on veut, on le laisse inchangé. Si ce n'est pas le cas, on lui ajoute 1 (à une exception près : si le nombre est égal à 255, on sera obligé de soustraire 1 pour éviter les débordements).

Reprenons le tableau donné en exemple ci-dessus et camouflons-y la lettre A, qui a le code ASCII 65, ce qui correspond à 01000001 en binaire :

No de pixel	1			2			3			
Couleurs	R	G	B	R	G	B	R	G	B	...
Image originale	255	255	255	153	219	5	102	0	201	...
Lettre « A »	0	1	0	0	0	0	0	1	...	...
Image modifiée	254	255	254	154	220	6	102	1	...	...

Récupération du texte

La récupération se fait en cinq étapes :

1. Récupérer le tableau des pixels décrivant l'image.
2. Remplacer un nombre pair par 0, un nombre impair par 1.
3. Grouper les bits par groupes de 8.
4. Convertir chaque octet en nombre décimal.
5. Écrire les caractères correspondant aux codes ASCII obtenus.

Exemple

Image originale

Image modifiée

Pixels modifiés

J'ai caché une fable de La Fontaine dans l'image d'un perroquet.

Il n'y a à l'œil nu aucune différence entre les deux premières images. Pourtant tout le bas de l'image a été modifié, comme le montre la troisième image. On pourra perfectionner la méthode en ne codant pas des pixels successifs, car cela facilite le repérage des images trafiquées.

Stéganalyse

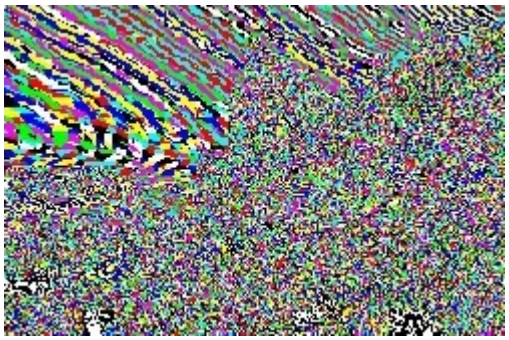
La stéganalyse est à la stéganographie ce que la cryptanalyse est à la cryptographie. Cette discipline cherche à détecter et à décrypter les messages cachés.

Apparemment, modifier les bits de poids faibles est totalement invisible. C'est vrai pour l'œil, mais pas pour les statistiques ! En effet, on pourrait penser que les valeurs du bit du poids faible sont uniformément réparties dans une image. Ce n'est pourtant pas le cas, car les capteurs des appareils numériques ou des scanners ont tendance à saturer certaines couleurs. Ainsi, un pixel de couleur blanc définie dans le système RGB sera toujours représentée par le triplet (255, 255, 255) et jamais (254, 253, 254), par exemple.

Pour s'en convaincre, on peut transformer l'image en remplaçant les nombres de chaque triplet par 255 s'ils sont impairs ou par 0 s'ils sont pairs. Par exemple, le pixel de couleur (134, 12, 251) prendra la couleur (0, 0, 255), c'est-à-dire bleu. Vous trouverez ci-après un exemple de ce que l'on obtient, tiré du livre de Peter Wayner, **Disappearing Cryptography**, [WAYN02], pp. 149-182.

Les huit couleurs de l'image de droite sont : blanc, noir, rouge, bleu, jaune, vert, magenta et cyan. Ce sont les huit couleurs obtenues en mélangeant de manière saturée les trois couleurs rouge, vert et bleu.

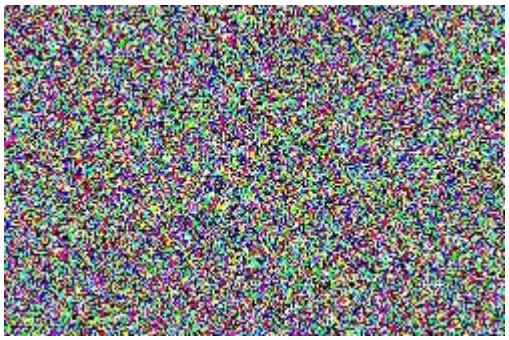
Image initiale



Couleurs obtenues selon le procédé expliqué ci-dessus

Dans l'image de gauche ci-dessous, on a ajouté un message aléatoire en modifiant le bit de poids faible (en donc en modifiant la parité de certains nombres). C'est invisible à l'œil nu, mais on voit sur l'image de droite que cette opération rend la répartition des couleurs plus uniforme.

Image trafiquée



Couleurs obtenues selon le procédé expliqué ci-dessus

Cette particularité permet de déceler quelles images pourraient contenir un message. On pourra plus tard essayer de les décrypter, ou, au pire, empêcher qu'elles arrivent à leur destinataire.

2.14. Cryptographie visuelle

Le concept de cryptologie visuelle a été proposé par **Moni Naor** et **Adi Shamir** en 1994 dans leur article « Visual Cryptography », dans *EUROCRYPT*, 1994, pp. 1-12.

L'idée est d'« additionner » deux images (l'originale et une image-clef). Une image digitalisée peut être décrite comme une suite de pixels (des points lumineux), chaque pixel ayant une couleur. Supposons pour simplifier que l'image est en niveaux de gris. Le niveau de gris sera représenté par exemple par un nombre entier entre 0 et 255 (0 : noir, 255 : blanc). Ces nombres sont codés dans l'ordinateur en binaire sur 8 bits (par ex.: 01001010=74). On peut « additionner » deux bits à l'aide de la fonction XOR (OU exclusif) donnée par le tableau ci-dessous :

XOR	0	1
0	0	1
1	1	0

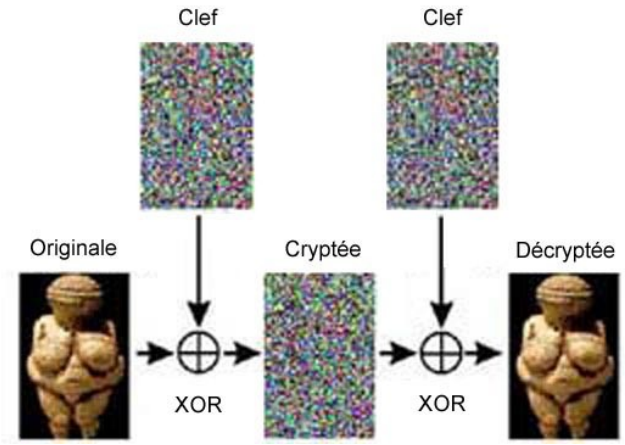
Ainsi, si le premier pixel de l'image originale est 01110011 et le premier pixel de l'image-clef 10100101, l'«addition» des deux sera :

1er pixel de l'image originale	0	1	1	1	0	0	1	1
1er pixel de l'image-clef	1	0	1	0	0	1	0	1
1er pixel de l'image brouillée	1	1	0	1	0	1	1	0

Le grand intérêt de cette méthode réside dans le fait que si l'on additionne l'image brouillée et l'image-clef, on retrouve l'image originale. Regardons ce qui se passe si l'on additionne le premier pixel de l'image brouillée au premier pixel de l'image-clef :

1er pixel de l'image brouillée	1	1	0	1	0	1	1	0
1er pixel de l'image-clef	1	0	1	0	0	1	0	1
1er pixel de l'image originale	0	1	1	1	0	0	1	1

Le schéma ci-dessous résume le processus de cryptement/décryptement. La même clef est utilisée pour crypter et décrypter. On dit que c'est un système symétrique.



Pourquoi ne faut-il pas utiliser deux fois la même image-clef ?

Avec cette manière de crypter des images, que l'on appelle technique du « masque jetable » (le masque étant l'image-clef), il faut impérativement n'utiliser l'image-clef qu'une seule fois. En effet, si l'adversaire intercepte deux images cryptées avec la même image-clef, voici ce qui se passe (« addition » a le même sens que ci-dessus) :

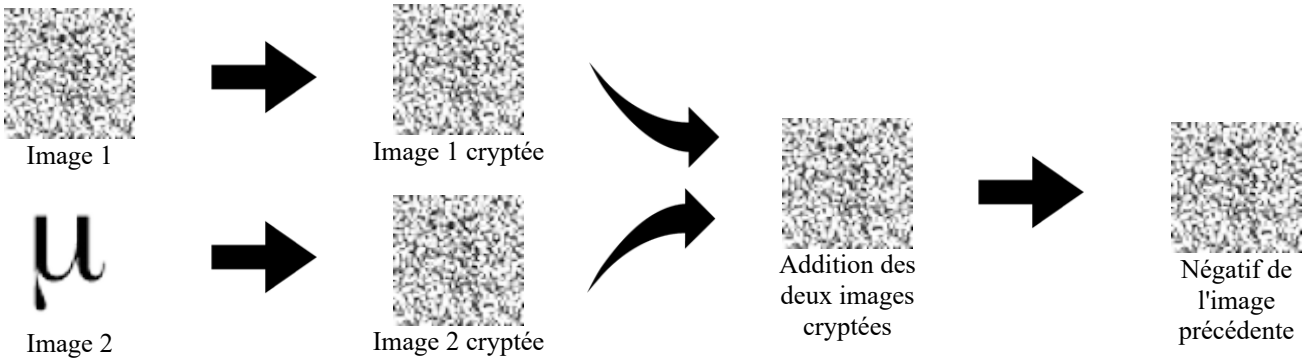
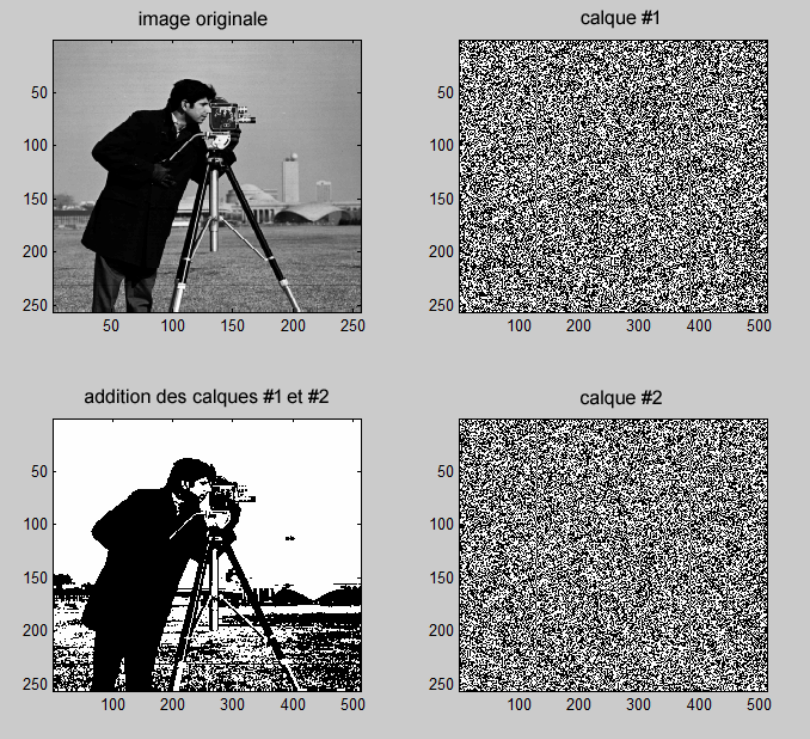
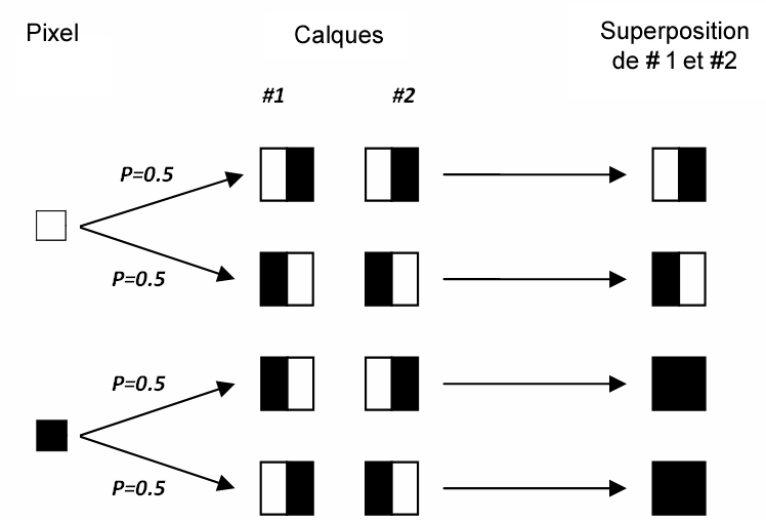


Image éclatée

On peut voir cette technique différemment en imaginant que l'image est en fait éclatée en deux calques (traduction approximative de *share* en anglais). Chacun des deux calques est illisible mais la superposition des deux donne une image complète.



Pour simplifier l'explication, prenons une image en noir et blanc de n x m pixels. Chaque pixel de l'image est soit blanc (0) soit noir (1). Pour éclater l'image en deux calques de taille $2n$ x $2m$, on procédera comme dans l'illustration ci-après :



Si le pixel est blanc, on choisira avec une probabilité $p = 1/2$ l'une des deux possibilités de le remplacer par un carré de 2 x 2 pixels. Si le pixel est noir, on fera de même.

Ici, la superposition (dernière colonne du schéma) n'est pas une addition XOR comme précédemment, mais un simple OR (OU inclusif).

OR	0	1
0	0	1
1	1	1

Il sera ensuite facile de retrouver l'image exacte de départ : si un carré 2 x 2 contient 2 pixels blancs, ce sera un pixel blanc. Si le carré 2 x 2 est entièrement noir, ce sera un pixel noir.

Il est à noter que l'on n'a pas besoin d'un ordinateur pour voir apparaître l'image. Si on imprime les calques sur deux transparents, puis qu'on les superpose en les alignant bien, l'image apparaîtra alors, mais dégradée (bruitée), car le OU opéré par l'œil laisse un bruit qui remplace le blanc de l'image secrète initiale.

Dans son article « Cryptographie visuelle », Pour la Science n° 416, juin 2012, **Jean-Paul Delahaye** explique comment exploser l'image en trois calques. L'image n'apparaîtra qu'en superposant les trois calques ; deux ne suffiront pas.

2.15. La stéganographie dans la littérature et l'art

Hypnerotomachia Poliphili

Hypnerotomachia Poliphili, en français, ***Songe de Poliphile***, rédigé en 1467 et imprimé à Venise en 1499, est un roman illustré italien écrit en un mélange de grec, de latin et d'italien dialectal.

Qualifié de l'un des « livres les plus beaux du monde », il est aussi l'un des plus mystérieux de la Renaissance.

Alde Manuce a imprimé ce livre à Venise en décembre 1499. L'auteur est anonyme, mais un acrostiche tend à faire attribuer l'œuvre à un certain **Francesco Colonna**, identifié traditionnellement avec le moine vénitien Francesco Colonna et plus récemment avec un autre Francesco Colonna, seigneur de Palestrina. En effet, on peut remarquer que la première lettrine[9] de chaque chapitre forme un message : « *Poliam frater Franciscus Columna peramavit* » (« Frère Francesco Colonna a aimé Polia intensément »).

POLIPHILO QVIVI NARRA,CHE GLI PARVE AN-
CORA DI DORMIRE,ET ALTRONDE IN SOMNO
RITROVARSE IN VNA CONVALLE,LAQVALE NEL
FINE ERA SERATA DE VNA MIRABILE CLAVSVRA
CVM VNA PORTENTOSA PYRAMIDE,DE ADMI-
RATIONE DIGNA,ET VNO EXCELSO OBELISCO DE
SOPRA.LAQVALE CVM DILIGENTIA ET PIACERE
SVBTILMENTE LA CONSIDEROE.

[9] Lors de l'écriture de ma thèse de doctorat, je m'étais aussi amusé à cacher des mots de cette façon. Essayez de les trouver ! https://www.apprendre-en-ligne.net/auteur/roso/SIGMA.PDF

Pantagruel, chapitre XXIV

Dans ce chapitre de *Pantagruel*, **Rabelais** fait une longue allusion aux encres invisibles :

Lettres que un messagier aporta à Pantagruel d'une dame de Paris, et l'exposition d'un mot escript en un aneau d'or.

Quand Pantagruel eut leue l'inscription, il feut bien esbahy, et, demandant au dict messagier le nom de celle qui l'avoit envoyé, ouvrit les lettres, et rien ne trouva dedans escript, mais seulement un aneau d'or, avecques un diament en table. Lors appella Panurge et luy monstra le cas.

A quoy Panurge luy dist que la fueille de papier estoit escripte, mais c'estoit par telle subtilité que l'on n'y veoit poinct d'escripture.

Et pour le sçavoir, la mist auprès du feu, pour veoir si l'escripture estoit faicte avec du sel ammoniac destrempé en eau[10].

Puis la mist dedans l'eau, pour sçavoir si la lettre estoit escripte du suc de tithymalle[11].

Puis la monstra à la chandelle, si elle estoit poinct escripte du jus de oignons blans.

Puis en frotta une partie d'huille de noix, pour veoir si elle estoit poinct escripte de lexif de figuier.

Puis en frotta une part de laict de femme allaictant sa fille première née, pour veoir si elle estoit poinct escripte de sang de rubettes[12].

Puis en frotta un coing de cendres d'un nic de arondelles, pour veoir si elle estoit escripte de rousée qu'on trouve dedans les pommes de Alicacabut.

Puis en frotta un aultre bout de la sanie des aureilles, pour veoir si elle estoit escripte de fiel de corbeau.

Puis les trempa en vinaigre, pour veoir si elle estoit escripte de laict de espurge.

Puis les gressa d'axunge de souris chauves, pour veoir si elle estoit escripte avec sperme de baleine qu'on appelle ambre gris.

Puis la mist tout doulcement dedans un bassin d'eau fresche et soubdain la tira, pour veoir si elle estoit escripte avecques alum de plume.[13]

Et, voyant qu'il n'y congnoissoit rien, appella le messagier et luy demanda :

« Compaing, la dame qui t'a icy envoyé t'a-elle poinct baillé de baston pour apporter », pensant que feust la finesse que mect Aule Gelle.[14]

Et le messagier luy respondit : « Non, Monsieur. »

Adoncques Panurge luy voulut faire raire les cheveulx, pour sçavoir si la dame avoit faict escripre avecques fort moret[15] sur sa teste rase ce qu'elle vouloit mander ; mais, voyant que ses cheveulx estoyent fort grand, il desista, considerant que en si peu de temps ses cheveulx n'eussent creuz si longs.[16]

Alors dist à Pantagruel :

« Maistre, par les vertuz Dieu, je n'y sçauroys que faire ny dire. Je ay employé, pour congnoistre si rien y a icy escript, une partie de ce que en met Messere Francesco di Nianto, le Thuscan, qui a escript la manière de lire lettres non apparentes, et ce que escript Zoroaster, *Peri Grammaton acriton,* et Calphurnius Bassus, *De Literis illegibilibus ;* mais je n'y voy rien, et croy qu'il n'y a aultre chose que l'aneau. Or le voyons. »[17]

Lors, le regardant, trouverent escrit par dedans en Hébrieu :

LAMAH HAZABTHANI.

Dont appellèrent Epistémon, luy demandant que c'estoit à dire. A quoy respondit que c'estoyent motz Hébraicques, signifians : *Pourquoy me as-tu laissé ?*

Dont soubdain réplicqua Panurge :

[10] Ce procédé figure dans le traité *Polygraphiae* de **Trithème** (1518).

[11] Variété d'euphorbe, dont le suc était utilisé pour la stéganographie par les Anciens (cf. **Pline l'Ancien**, *Histoire naturelle*, Livre XXVI, Ch. XXXIX)

[12] Crapauds

[13] Une partie de cet épisode se réfère à des faits exacts, l'autre n'est que pure invention. En effet, l'ammoniaque, l'oignon, l'alun, la sève du tithymale sont des recettes valables, tandis que le sang de crapaud, le cérumen, la graisse de chauve-souris ne font que railler les étranges formules des charlatans de l'époque.

[14] Le bâton est, bien sûr, la scytale des Lacédémoniens, décrite par Aulu-Gelle dans les *Nuits attiques*.

[15] Sorte d'encre.

[16] L'allusion à un message tatoué sur un crâne rasé s'inspire du fameux récit d'Hérodote.

[17] Les trois ouvrages cités dans ce passage n'existent pas.

« J'entens le cas. Voyez vous ce dyament ? C'est un dyament faulx. Telle est doncques l'exposition de ce que veult dire la dame :

Dy, amant faulx, pourquoy me as-tu laissée ? »

[...]

Le scarabée d'or

Dans sa nouvelle *Le Scarabée d'Or* (j'en reparlerai beaucoup plus en détails dans le § 5.11), **Edgar Allan Poe** donne deux recettes d'encre invisible qui apparaissent avec la chaleur :

- « ...le safre, digéré dans de l'eau régale (mélange d'acide chlorhydrique et d'acide nitrique concentrés) et délayé dans quatre fois son poids d'eau; il en résulte une teinte verte. »
- « Le régule de cobalt, dissous dans l'esprit de nitre, donne une couleur rouge. »

La première lettre

Vous voyez ci-contre une illustration de **Rudyard Kipling** pour *The first letter*, une des histoires de son célèbre livre pour enfants *Just So Stories*.

Cette image montre une défense en ivoire sur laquelle est gravée des dessins racontant l'histoire d'une jeune fille nommée Taffimai. Kipling dit que les étranges symboles sur les côtés sont des lettres runiques magiques, mais il s'agit en fait d'un alphabet. Pourrez-vous déchiffrer ces symboles ?

Deux indications pour vous aider :

- Il y a quelques bizarreries dans ce texte : U signifie YOU, W est supprimé ou remplacé par OU, F remplace V et I est utilisé à la place de Y. De plus, A, G, O et T ont deux symboles de substitution et H en a trois.
- Le texte sur la partie gauche commence ainsi :

  « This is the story of Taffimai, all written out on an old tusk... »

Cryptogramme 2.1

Une carte de Florentin Garraux

Florentin Garraux (1859-1950) tenait un négoce de mercerie et épicerie à Moutier (Suisse) de 1899 à 1927. Il se définissait comme un « peinturleur » et dessina plusieurs milliers de cartes, toutes plus belles les unes que les autres, qu'il envoyait à ses amis.

Dans une exposition qui lui était consacrée en 2017, j'ai remarqué la carte ci-contre, qui m'a fait penser à « La première lettre » de Kipling.

On remarque sous le dessin un curieux texte, écrit à première vue dans une langue exotique. Pourtant, ce n'est pas le cas.

Saurez-vous le décrypter ?

Les hommes dansants

Les Hommes dansants, aussi traduite *Les Danseurs* (*The Adventure of the Dancing Men* en version originale), est l'une des cinquante-six nouvelles d'**Arthur Conan Doyle** mettant en scène le détective Sherlock Holmes. L'intrigue de la nouvelle *Les Hommes dansants* repose sur une énigme cryptographique.

Dans cette nouvelle, Sherlock Holmes réussit à briser le code des messages chiffrés qui terrifient la femme de son client. Ces messages sont composés de suites de symboles différents, en forme de personnages agitant les bras et les jambes, parfois munis de petits drapeaux : les « hommes dansants ».

Sherlock Holmes parvient à décrypter ces séries de dessins en étudiant les fréquences d'apparition de chaque personnage, selon la méthode de l'analyse fréquentielle (voir § 5.4). Ce cryptogramme est une substitution monoalphabétique (voir chapitre 5) : chaque personnage représente une lettre. Les drapeaux indiquent la fin d'un mot.

Pour casser ce chiffre, Holmes étudia plusieurs cryptogrammes et utilisa l'analyse des fréquence pour identifier le E. Il parvint ensuite à identifier le mot « never » dans un cryptogramme ne comportant que cinq lettres, ce qui lui fournit trois nouvelles correspondances. En utilisant ensuite quelques mots probables relatifs à l'enquête qu'il menait, il parvint à reconstituer l'alphabet de chiffrement. La traduction du cryptogramme ci-dessus est « am here Abe Slaney ».

L'intérêt de ce chiffre est sa discrétion : utilisé dans des messages gribouillés sur des murs ou des bouts de papier, il passe inaperçu car on peut le prendre pour un dessin d'enfant. C'est donc une forme de stéganographie.

Image cachée dans la tranche d'un livre

Certains livres contiennent une image cachée qui n'apparaît qu'en décalant les pages de sorte que la tranche soit oblique.

Lanfeust de Troy

La bande dessinée *Lanfeust de Troy*, écrite par **Christophe Arleston** et dessinée par **Didier Tarquin**, regorge de messages stéganographiques.

Par exemple dans le tome 3, page 40, au milieu d'un invraisemblable bric-à-brac, on peut voir un tas de feuilles où il est écrit en tout petit : « Dix autres séries de BD se cachent sur ce dessin. À toi de trouver les indices. Solution dans une des pages suivantes ».

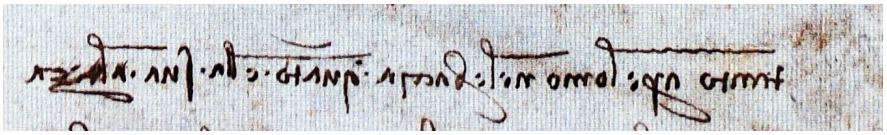
Ces textes minuscules apparaissent dans d'autres albums de la série.

Écriture spéculaire

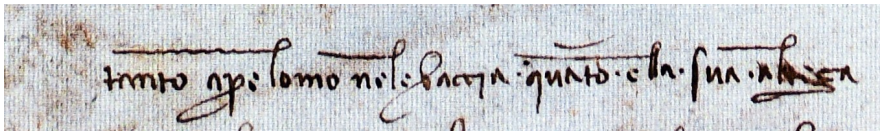
Voici une affiche que l'on trouvait dans les toilettes publiques. Au premier regard, on croit à un slogan écrit en russe. Pourtant, en se lavant les mains et en voyant l'affiche dans un miroir, on voyait apparaître un message en anglais : *Real men don't drink and drive.*

Ce système d'écriture en miroir, que l'on qualifie de spéculaire, était déjà utilisé par **Léonard de Vinci** (1452-1519). En effet, pour tenir ses écrits à l'abri des regards indiscrets, il avait l'habitude d'écrire de droite à gauche. Évidemment, ce procédé n'offre qu'une très faible protection, mais à son époque c'était assez efficace, puisque peu de gens savaient lire.

Ce procédé est notamment utilisé sur les notes de son célèbre dessin : l'Homme de Vitruve. Observons un détail :



Texte original



Texte « retourné »

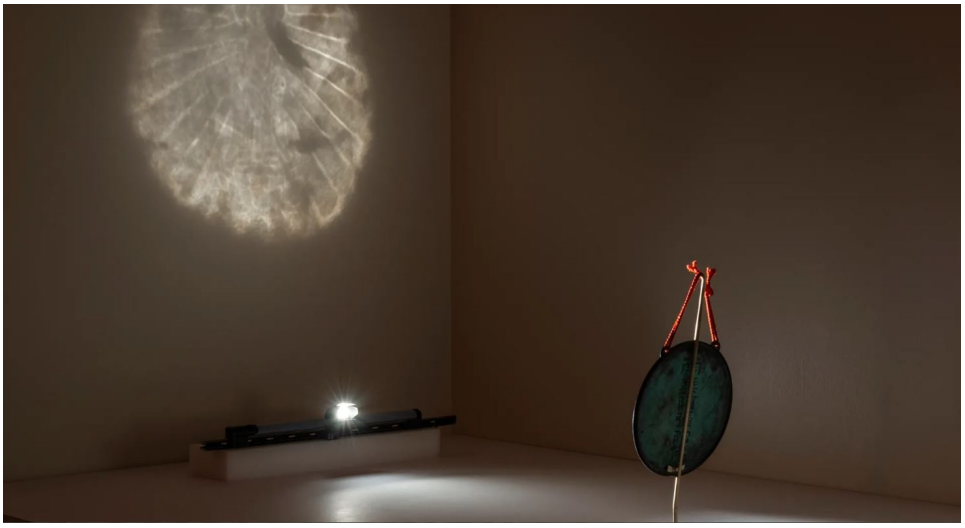
On peut lire en toscan « Tanto apre l'omo nelle braccia · quato · è la · sua altezza ». En français « La longueur des bras étendus d'un homme est égale à sa taille ».

Une autre publicité pour un skatepark couvert (à gauche), utilise l'écriture spéculaire. Cette fois-ci on déchiffre le panneau en le lisant dans les reflets d'une flaque d'eau. Quelle merveilleuse idée !

Miroirs magiques

Depuis plus de 50 ans, le musée d'Arts de Cincinnati (Ohio, États-Unis) conservait dans sa réserve un petit miroir en bronze. Originaire d'Asie de l'Est, l'objet était plutôt insignifiant. **Hou-Mei Sung**, conservatrice au musée, a remarqué qu'il ressemblait à certains « miroirs magiques » de la période Edo, au Japon.

Ces très rares artefacts révèlent, avec un éclairage particulier, des dessins qui se projettent sur un mur. Après quelques expériences pour trouver le bon éclairage, c'est un net dessin de Bouddha qui a fait son apparition. Derrière le miroir, une inscription indique qu'il s'agit d'Amitabha, une figure importante dans le bouddhisme d'Asie de l'Est.



Le miroir avec son reflet, exposé depuis le 23 juillet 2022 au Musée des Arts de Cincinnati
Rob Deslongchamps/Cincinnati Art Museum

Le reflet du « miroir magique » Bouddhiste
Rob Deslongchamps/Cincinnati Art Museum

Cette découverte extraordinaire s'ajoute à la très réduite collection de « miroirs magiques » présents dans le monde. D'après la conservatrice, il n'y en aurait que trois qui dépeindraient des Bouddha, dont un au MET de New York.

Celui-ci, de 8,5 centimètres de diamètre, était probablement accroché dans un temple ou dans la maison d'une famille noble. Le musée est encore en train d'enquêter sur son origine, mais pencherait sur la Chine ou le Japon.

Ces petits objets mystérieux existeraient depuis 2000 ans. Originaires de Chine, ils nécessitent une technique particulièrement raffinée de sculpture sur bronze. Les scientifiques d'aujourd'hui ne comprennent toujours pas comment les artisans de l'époque faisaient...

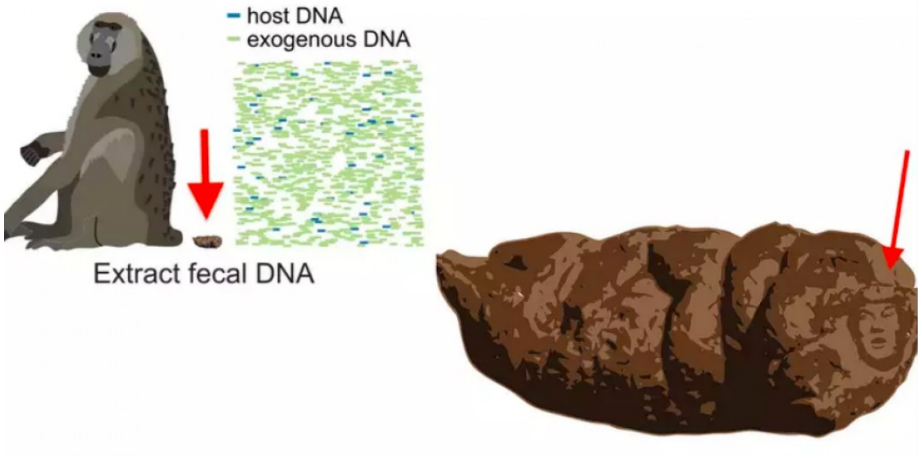
Images cachées

Où sont cachés les habitants du moulin ? On cherche des humains et des animaux…

Couverture de « Jeu et Stratégie n° 28 », août-septembre 1984

La littérature scientifique n'est pas en reste. En janvier 2018, deux scientifiques ont publié un article sur une technique permettant de faciliter le séquençage génétique d'animaux à partir de leurs excréments. L'étude[18], « *Methylation-based enrichment facilitates low-cost, noninvasive genomic scale sequencing of populations from feces* », publiée dans la revue en ligne *Scientific Reports*, introduit une nouvelle technique pour isoler l'ADN de l'animal de celui des autres organismes (notamment des bactéries), contenus dans la matière fécale.

Onze mois plus tard, cet obscur papier est soudainement devenu très populaire sur Facebook et Twitter : quelqu'un a en effet découvert qu'en zoomant sur l'étron de babouin utilisé pour illustrer l'article, on pouvait distinguer le visage de **Donald Trump**. Comment a-t-il eu l'idée de faire ça ? L'histoire ne le dit pas...



La direction de la revue *Scientific Reports* a rapidement ajouté une note en bas de l'article :

Change history

14 December 2018 Editors' Note: The editors have become aware of unusual aspects to the 'Extract fecal DNA' illustration in figure 1. We are investigating, and appropriate editorial action will be taken once the matter is resolved.

19 December 2018 In the original version of this Article, there were unusual aspects to the 'Extract fecal DNA' illustration in figure 1. These features have been removed.

L'illustration a été retirée le 19 décembre, mais elle avait déjà été préservée par des fans sur Internet. Plusieurs médias ont tenté de contacter les deux jeunes auteurs de la blague, **Kenneth Chiou** et **Christina Bergey**, mais ils n'ont pas répondu.

Aviez-vous déjà remarqué l'ours caché dans le logo de la barre chocolatée **Toblerone** ? À première vue, seule la montagne représentant le Cervin apparaît. Pourtant, on peut aussi déceler un ours qui se cache au creux de la montagne. Cet ours est le symbole de Berne, la ville où le fondateur Mathias Tobler s'est installé à ses débuts.

[18] https://www.nature.com/articles/s41598-018-20427-9

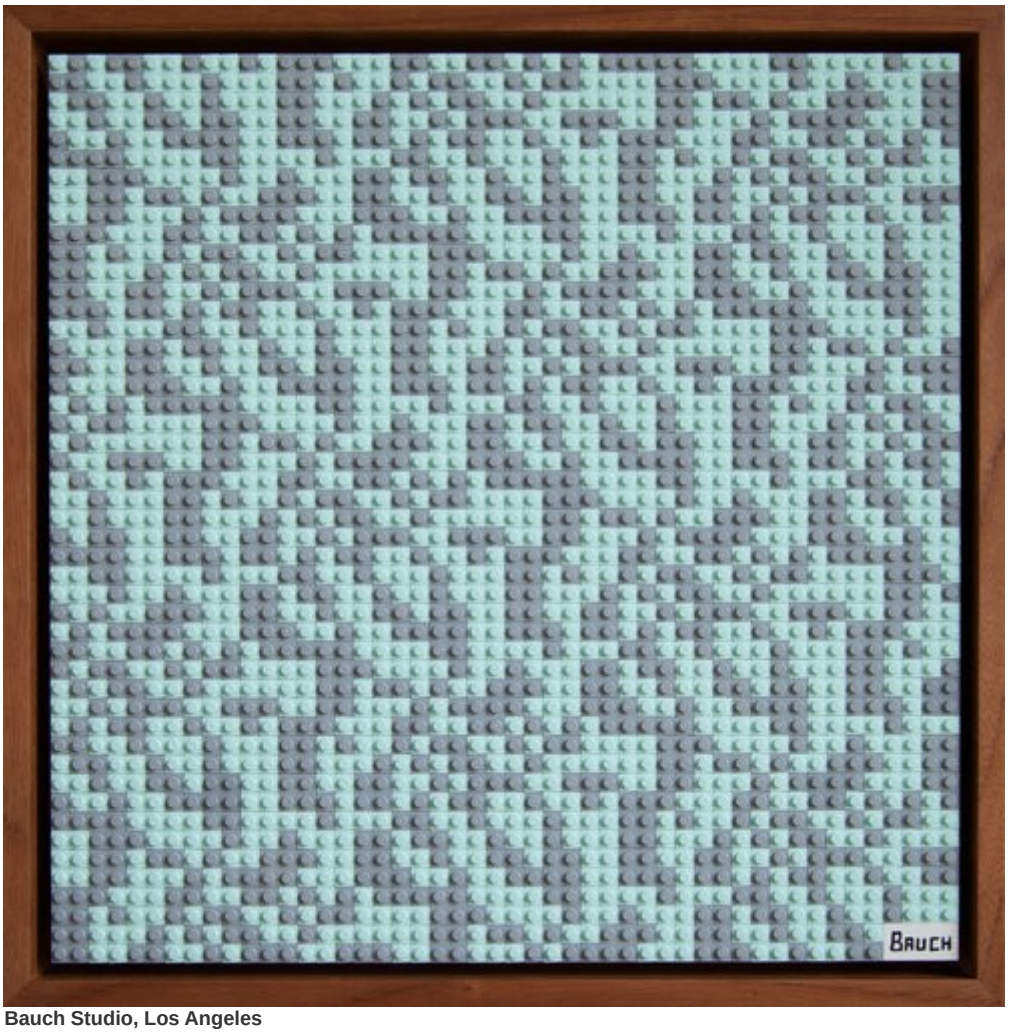
Les mosaïques d'Andy Bauch

La série de tableaux d'**Andy Bauch** intitulée « New Money »[19] combine l'art et la technologie de la cryptomonnaie en cachant des codes abstraits dans mosaïques faites avec des carrés Lego. Dans ces tableaux sont dissimulées des clefs privées de portefeuilles contenant jusqu'à 9000$ en cryptomonnaie. L'achat d'une œuvre donnée ne signifie pas que vous devenez propriétaire d'une clef privée, car quiconque décrypte le code pourra prendre l'argent pour lui-même.

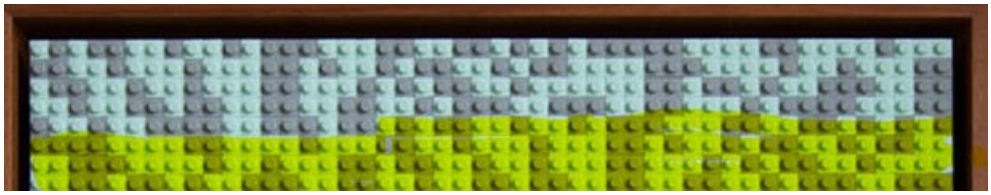
L'exposition s'est déroulée au Castelli Art Space à Los Angeles les 23 et 25 mars 2018. Pour ce projet artistique particulier, Bauch a commencé à acheter diverses cryptomonnaies en 2016. Il a ensuite utilisé leur clef privée pour générer un motif abstrait.

Ils ne sont pas très difficiles à décoder.

Prenons le tableau ci-après comme exemple.



En observant attentivement, on remarque un motif de 210 carrés qui se répète :



[19] https://andybauch.com/

En interprétant les 210 premières unités comme des bits (clair = 1, foncé = 0), on obtient la chaîne binaire suivante :

```
1010011 0110100 0111001 1001010 1000001 1110011 1101110 0110111 0111001
0110100 1101001 1110001 1110110 1110010 0110110 1110011 1010100 1101111
1100100 1011000 1100110 1100100 1100110 0110100 0110001 1001110 1000011
1000110 1100001 1000100
```

Chacun des blocs est un nombre binaire que l'on peut écrire en décimal :

```
 83  52  57  74  65 115 110 55  57
 52 105 113 118 114  54 115 84 111
100  88 102 100 102  52  49 78  67
 70  97  68
```

Ces nombres correspondent à un caractère du code ASCII, ce qui donne :

S49JAsn794iqvr6sTodXfdf41NCFaD

Cette suite de caractères est une clef privée, qui peut être convertie en une adresse Bitcoin en se rendant sur un site comme WalletGenerator.net.

On obtient l'adresse publique de portefeuille BitCoin suivante :

1NmxAV1ze28U4Uuqg2fH1JTB8NtWKvTyhM

Je ne vais pas expliquer en détails comment fonctionnent les bitcoins, bien qu'il y ait une relation très étroite entre les monnaies virtuelles et la cryptographie. Sachez simplement que c'est la clef privée qui vous définit comme le propriétaire du bitcoin. Grâce à elle, vous pouvez générer une clef publique. Il existe une relation mathématique entre la clef privée et la clef publique, qui permet de vérifier une signature créée avec la clef privée. Alors qu'il est facile et rapide de calculer la clef publique à partir de la clef privée, l'inverse est impossible. Je reparlerai de ce concept de clef publique et clef privée au chapitre 11.

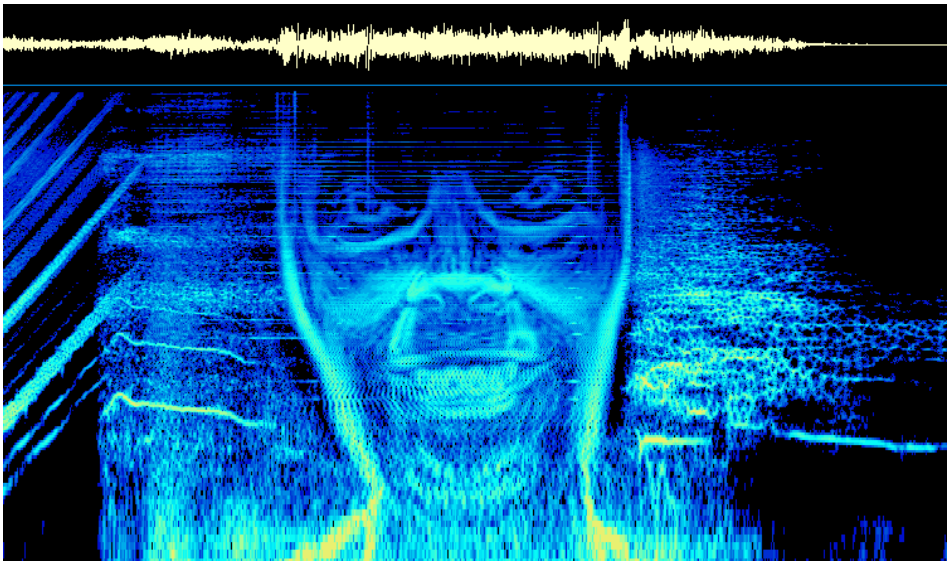
Une adresse bitcoin est un *hash* d'une clef publique. Un hash est une fonction mathématique permettant de créer un condensé d'une donnée dans un format constant mais irréversible. Si vous avez une

clef publique et que vous calculez le hash de cette valeur, vous obtiendrez toujours les mêmes 160 caractères et dans le même ordre. Cependant, si vous avez les 160 caractères vous ne pourrez pas retrouver la clef publique. C'est pourquoi quand on a uniquement une adresse bitcoin il est impossible de retrouver la clef publique, mais si on a la clef publique, il est très facile de calculer l'adresse bitcoin.

Le visage d'Aphex

Un spectrographe est un instrument ou un programme utilisé pour visualiser le spectre sonore. En outre, il existe également des programmes qui permettent de convertir facilement n'importe quelle image en un fichier audio.

Les musiciens peuvent alors prendre ces fichiers « image to audio », les incruster dans une piste. Si vous exécutez ce fichier audio à travers un spectrographe, vous verrez soudainement apparaître des images. La plus célèbre d'entre elles est tirée de la chanson « [Equation] » d'**Aphex Twin**, présentée ci-après.



Un message du groupe BTS

BTS, aussi connu sous le nom **Bangtan Sonyeondan** ou **Bangtan Boys**, est un boys band sud-coréen originaire de Séoul. Sur le compte Instagram[20] @6c_6f_73_74_20_75_73_65_72 (code hexadécimal signifiant « Lost user »), ce groupe a posté le message suivant :

```
T737362764636276227747363736472637372746282 87H84838293738274927482827482827491 0
1E7572918473729284729284729274 8Y___754829433438382 7HA7582019747491014739194729 1
748202742810V8682939584747920284829294719E___6473828472843U747282847384 74S___74
7274737374791L0103910382019301092929190648291047291947294719 4719C75829194747292
65829K648291047483919E637194729184819D___648283618582974U64829286582P___
```

Cela reprend le principe de la grille de Cardan, un procédé du 16ème siècle. Le message est noyé dans un flot de caractères sans signification, ici les chiffres. En effet, si on ne lit que les lettres, le message devient : « THEY HAVE US LOCKED UP ».

Comme quoi, même à l'ère d'Internet, le bonnes vieilles méthodes peuvent encore être utilisées.

[20] https://www.instagram.com/6c_6f_73_74_20_75_73_65_72/

Quand les IA créent des messages subliminaux

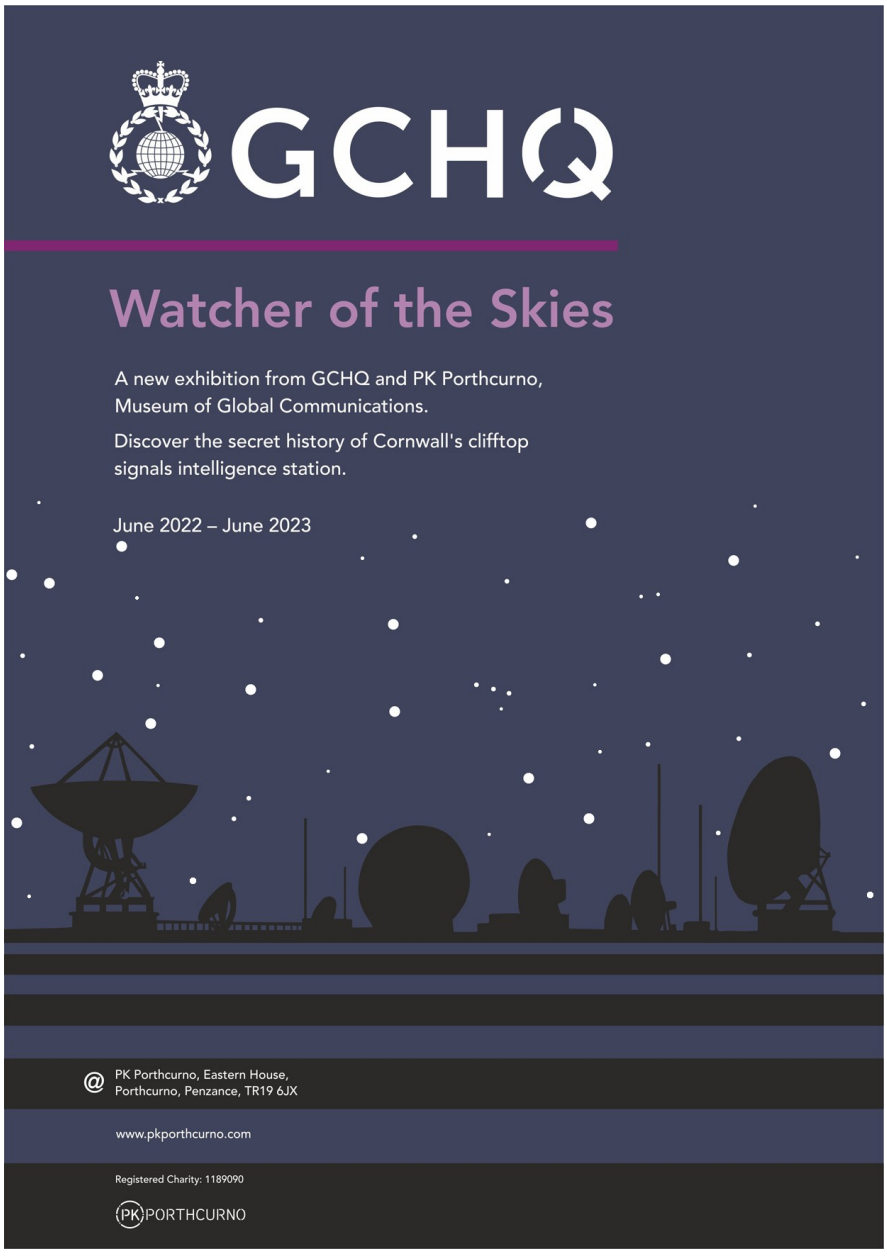
Depuis 2023, les IA génératives comme Midjourney sont capables de créer des images contenant un message subliminal. Pour le voir, il faut cligner des yeux ou s'éloigner de l'image.

Les images ci-après proviennent du web. Malheureusement, les auteurs ne sont pas cités.

2.16. Les mains dans le cambouis

Les textes et les images ci-dessous renferment des messages cachés. À vous de les découvrir ! Indices et solutions dans l'annexe A.

Cryptogramme 2.2



Cryptogramme 2.3

Jet-stream qui m'emporte loin de moi
tabou que je fais voler en éclat
immaculée comme les premières neiges
ectoplasme vampirisant mes nuits

ombre qui luit
mentholée et fraîche
unique et taquine korrigane
palpitant dans mon corps ivre
insensé nectar
démiurge mélomane
piquant violemment ses dards
cendre qui me brûle
magicienne que j'adule
mystérieux troubadour
riant de ce rioja qui m'enivre
amarante de mes amours

Cryptogramme 2.4

Baiser maladroit de deux écorchés
Noyant dans son désir sacré
Les coquelicots qui soliloquent
Attisant le brasier de nos sens
Haletant comme une hallucination
Doucereux doute hyperbolique
Mesquine mescaline de ventriloque
Ivoire rose de mon imagination
Douceur d'un été d'automne précoce
Silence si long de six lances
Zibeline glissant entre mes doigts d'écorce
Hiver d'un printemps prospère
Lacet de nos lèvres mélancoliques
Douce heure qui reviendra j'espère

Cryptogramme 2.5

Extrait de la nouvelle d'Arthur Conan Doyle *Le « Gloria-Scott »*.

> – J'ai ici quelques papiers, me dit mon ami Sherlock Holmes un soir d'hiver où nous étions assis de chaque côté de la cheminée, qui selon moi mériteraient que vous y jetiez un coup d'œil. Il s'agit des documents qui se rapportent à l'affaire extraordinaire du Gloria-Scott : par exemple le message qui a foudroyé d'horreur le juge de paix Trevor quand il l'a lu.
>
> D'un tiroir, il avait exhumé une petite boîte décolorée ; après en avoir défait le ruban, il me tendit un court billet griffonné sur une demi-feuille de papier ardoisé. En voici le texte :
>
> > *« Plus de difficultés : rien comme gibier à Londres pour faire la concurrence. Hudson ton représentant a très bien vendu les faisans, la faisane et la mèche de fouet. Ta perdrix rouge seule a la chance de pouvoir quitter cette semaine l'élevage d'Angleterre. »*

Cryptogramme 2.6

Pancarte vue lors d'une manifestation en France :

2.17. Références

Livres

[BAUE02] Bauer F. L., **Decrypted Secrets**, 3rd edition, Springer, 2002

[BREM??] Brémond Charles, **Les écritures secrètes et les encres mystérieuses dites sympathiques**, Éd. Albin Michel, Paris, sans date (début du 20e siècle)

[CART38] Général Cartier, **Un problème de Cryptographie et d'Histoire**, Mercure de France, Paris, 1938 (4ème édition)

[CHEL97] Chély Pierre, **Méthode originale d'écriture secrète**, Guy Trédaniel éditeur, 1997

[JOLI74] Joliet Charles, **Les écritures secrètes dévoilées**, E. Dentu éditeur, Paris, 1874

[GARD84] Gardner Martin, **Codes, ciphers and secret writing**, Unabridged Dover, 1984,

[KAHN80] Kahn David, **La guerre des codes secrets**, InterEditions, 1980, pp. 359-364

[KLEI07] Klein Andreas, **Visuelle Kryptographie**, Springer, 2007

[LAFF68] Laffin John, **Petit code des codes secrets (codes et chiffres)**, Dargaud, 1968

[SCHM09] Schmeh Klaus, **Versteckte Botschaften: Die faszinierende Geschichte der Steganographie**, Heise, 2009

[SPEC24] Speckman H. A. W., **Les Méthodes de Cryptographie de Francis Bacon**, Extrait du Mercure de France no 628, Paris, 1924

[VIGE86] Vigenère Blaise (de), **Traicté des chiffres**, Paris 1586

[WAYN02] Wayner Peter, **Disappearing Cryptography**, Morgan Kauffman Publishers, 2002

[YARD35] Yardley Herbert O., **Le cabinet noir américain**, éd. de la nouvelle revue critique, 1935

[ZIMH48] Zim Herbert S., **Codes & secret writing,** Pan Book Limited, 1975 (1ère édition 1948)

Sites

- Bastwood, « The Aphex Face », <http://www.bastwood.com/?page_id=10>
- Cahya Prihandoko Antonius, « Visual Cryptography », <https://antoniuscpilkom.wordpress.com/lecture-notes/cryptography/visual-cryptography/>
- Chang Xiao, « FontCode: Embedding Information in Text Documents using Glyph Perturbation », <https://www.youtube.com/watch?time_continue=28&v=dejrBf9jW24>
- Instant Culture, « L'écriture en miroir de Léonard De Vinci », <https://www.instantculture.fr/2020/05/10/lecriture-en-miroir-de-leonard-de-vinci/>
- Lorain Pierre, « Le Chiffre », <http://codekeeper.free.fr/histoire.html>
- R. Marie, « Les tatouages de Prison Break décryptés », <http://marienightandday.blogspot.ch/2014/02/les-tatouages-de-prison-break-decryptes.html>
- Schmeh Klaus**,** « Andy Bauch's Lego code is broken », <http://scienceblogs.de/klausis-krypto-kolumne/2018/04/24/andy-bauchs-lego-code-is-broken/>
- Schmeh Klaus**,** « New information about the yellow dots code », <http://scienceblogs.de/klausis-krypto-kolumne/2018/07/01/new-information-about-the-yellow-dots-code/>
- Schmeh Klaus**, «** The Darknet of the Eighties », <http://scienceblogs.de/klausis-krypto-kolumne/2018/02/07/the-darknet-of-the-eighties/>
- Schmeh Klaus**, «** William Friedman's hidden messages », <http://scienceblogs.de/klausis-krypto-kolumne/2016/12/16/william-friedmans-hidden-messages/>
- Schmeh Klaus**,** « Five more accrostics », <http://scienceblogs.de/klausis-krypto-kolumne/2017/08/23/five-more-accrostics/>

Articles

- Buck Peter, Reverse Engineering the Machine Identification Code, juin 2018
- Chang Xiao, Cheng Zhang, Changxi Zheng, FontCode : Embedding Information in Text Documents using Glyph Perturbation, Columbia University, ACM Transactions on Graphics, Vol. 1, No. 1, Article 1. Publication date : January 2016
- Delahaye J.-P., Information noyée, information cachée, Pour la Science n° 229, novembre 1996
- Delahaye J.-P. , Cryptographie visuelle, Pour la Science n° 416, juin 2012
- Les chimistes écrivent aux chimistes, Université de Liège, Département de Chimie
- Robert McMillan, *Lyrics Site Accuses Google of Lifting Its Content*, The Wall Street Journal, 16 juin 2019
- Sarah Ziaï, *Un « miroir magique » révèle son extraordinaire secret enfoui depuis des années*, Vanity Fair, 2 août 2022

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Y

Z