



## Un smiley vieux de 3700 ans!

Dans notre numéro 39, nous présentons la plus ancienne version du "Penseur", dont Rodin a rendu la pause mondialement célèbre. Aujourd'hui, c'est le plus ancien "Smiley" que nous évoquons, en cette période de fêtes où le sourire est de rigueur!

Car le smiley ne date pas du 17e siècle, comme certains le pensaient, l'attribuant à un juriste slovaque ou à Robert Herrick, un poète anglais!



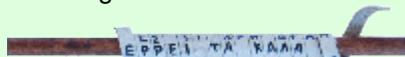
Celui-ci date de 1800 av. J.-C. et a été trouvé sur une cruche en terre cuite enfouie dans une tombe hittite, lors de fouilles conduites par une équipe italo-turque à Karkemish (une cité antique où l'on traversait autrefois l'Euphrate, aujourd'hui à la frontière de la Turquie et de la Syrie).

Il ne peut s'agir d'un canular, car des racines de micro-végétaux anciens se sont posées sur la surface du récipient ET sur la marque peinte, qui est donc d'origine.

Nous remercions pour cette information M. Nicolò Marchetti, professeur à l'Université de Bologne.

## Codes secrets: La scytale

Ce procédé, utilisé par les Spartiates dès le 5e siècle av. J.-C. est souvent cité comme étant le premier vrai système de codage. Il est simple: on enroule une bande de cuir en hélice autour d'un bâton (la scytale), et on écrit le message sur le cylindre de cuir ainsi constitué. Une fois le ruban déroulé, le message est illisible.



Le destinataire devra l'enrouler autour d'un autre bâton de même diamètre pour le lire aisément. Astucieux... Mais en supposant qu'on peut écrire 5 caractères sur la circonférence du bâton, il suffit en fait de lire une lettre, d'en sauter 4, d'en lire une, etc.



Bonnes fêtes et meilleurs vœux pour une excellente année 2018

[www.AnticoPédie.fr](http://www.AnticoPédie.fr)

## Les messages secrets dans l'Antiquité

Nombreuses sont les publications consacrées aux messages secrets, et beaucoup commencent par un historique qui évoque l'Antiquité. Mais ce sont toujours les mêmes exemples qui y sont cités et, sans les oublier, nous allons tenter de compléter un peu cela!

### Les premiers pas

De tous temps, les peuples ont eu besoin de communiquer entre eux discrètement, sans éveiller les soupçons de leurs ennemis ou de leurs gibiers, mais aussi parfois de leurs proches: tout n'est pas toujours avouable...

Quoi de plus naturel alors que d'employer en silence des gestes convenus ou au contraire, des cris sonores dont le sens échapperait aux oreilles indiscrettes?

A mesure que se bâtissaient les empires, il fallait diffuser des messages à grande distance, et c'est ici qu'interviennent les deux principales techniques:

- ◆ la cryptographie, dans lequel le message est visible mais inintelligible (par exemple un texte codé),
- ◆ la stéganographie qui, mieux encore, dissimule l'existence même d'un message (par exemple l'encre sympathique).

Au 4e siècle av. J.-C., le grec Enée le Tacticien (Aineias Taktikos, en latin Aeneas Tacticus), connu comme auteur de traités sur les techniques militaires (dont la "Poliorcétique", la science du siège des cités) expose une vingtaine de stratagèmes astucieux pour acheminer discrètement des messages.

### Avant l'alphabet

Lorsqu'on parle aujourd'hui d'un message secret, on pense naturellement qu'il s'agit d'un texte écrit avec notre alphabet, dont les lettres ont été altérées pour le rendre incompréhensible. Ce qui suppose déjà l'existence d'un alphabet.

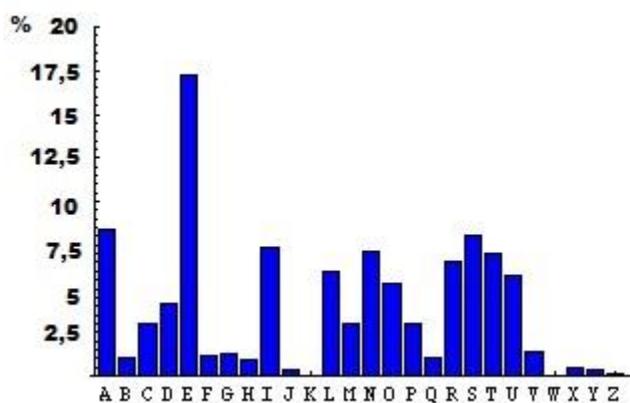
Comment faisait-on auparavant? Pas facile de chiffrer des hiéroglyphes égyptiens ou des cunéiformes mésopotamiens... Et pourtant, nécessité oblige, on note quelques exemples célèbres (ci-contre).

### Le cryptage des textes alphabétiques

Lorsque les écritures alphabétiques apparaissent, même si les méthodes antérieures restent en usage, les rédacteurs en viennent logiquement à une nouvelle solution: il suffit de remplacer chaque lettre du texte par... autre chose.

Au plus simple, on peut remplacer chaque lettre par une autre, ou par un graphisme différent. Cette technique a été utilisée pendant toute l'Antiquité, avec de nombreuses variantes.

Aujourd'hui, même un collégien pourrait venir à bout d'un tel code: si le texte est rédigé en français, il est facile d'identifier d'abord le E (la lettre la plus fréquente), puis les autres lettres de proche en proche selon leur fréquence statistique.



Fréquence d'emploi des lettres en français. On note que 17% des lettres d'un texte sont un E...

Pourtant, cette idée d'examiner la fréquence des signes n'apparaît qu'au 9e siècle de notre ère, et c'est le philosophe arabe Al-Kindi, versé dans la littérature comme dans l'arithmétique, qui la met en pratique.

Les Grecs et les Romains ne sont pas allés si loin, et il faut croire que la substitution d'une lettre à une autre était suffisante, puisque les indiscrets qui pouvaient tomber sur le message savaient généralement à peine lire.

### Coder n'est pas forcément dissimuler

De nos jours, le code informatique qui représente chaque lettre a simplement pour but de pouvoir la transmettre sous forme de signaux numériques. Eh bien, c'était déjà le cas dès l'époque antique, où les messages parcouraient d'énormes distances.

Les Grecs ont employé des méthodes de "télétransmission" similaires pour communiquer des messages écrits, en agitant de jour des fanions, de nuit des torches enflammées. Un code confidentiel certes, mais surtout pratique et rapide! A la fin du 18e siècle, le "télégraphe Chappe" ne fonctionnait pas très différemment...

## Codes secrets: Les origines

Le plus ancien document secret connu est une tablette cunéiforme en argile trouvée en Irak, oeuvre d'un potier babylonien. Il y avait noté le procédé qui faisait son succès. Il avait supprimé des signes et modifié l'orthographe des mots. Ce texte a été déchiffré...



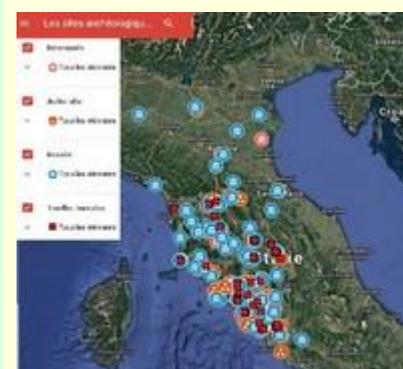
Bien sûr, certains textes antiques restent inintelligibles, comme le disque de Phaistos. Cachaient-ils pour autant des secrets?

En Egypte, on a trouvé, sur une tombe de la même époque, des inscriptions comportant des hiéroglyphes modifiés, apparemment pour en compliquer la lecture. Et selon quelques auteurs, les Egyptiens connaissaient déjà l'encre invisible (encre sympathique).

## L'aviez-vous vu?

Après les cartes des musées et sites archéologiques de France et de Grèce, nous proposons une **Carte interactive des sites archéologiques étrusques et des musées d'Etrurie.**

Cliquez ici



400 musées et sites à visiter, localisés précisément (car il n'est pas toujours facile de trouver une tombe dans une forêt...).



## À bientôt sur nos pages!

Toutes vos remarques et suggestions sont bienvenues!



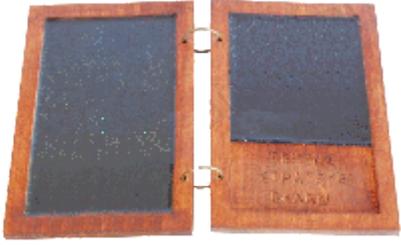
**Contactez-nous,** suivez-nous sur les réseaux sociaux



et retrouvez tous nos éditos et articles précédents sur



## Les astuces d'Enée le Tacticien



◆ Sachant que les lettres sont souvent écrites sur des tablettes enduites de cire (un procédé qui deviendra très courant à Rome), on grave le vrai message sur le bois de la tablette, que l'on recouvre ensuite de cire avant d'y écrire un message banal (image: K. Kotsanas).

◆ On écrit une lettre banale, mais il ne faut lire que les caractères marqués d'un signe, un petit point discret.

◆ On envoie un messenger chargé de réciter un message, mais le vrai message est caché à son insu dans ses vêtements ou dans le harnachement de son cheval.

◆ On peut enrouler le message écrit sur une feuille de plomb, de manière à former une boucle d'oreille qu'une femme élégante portera.

◆ Enée cite le cas d'Histiaeus qui, voulant avertir Aristagoras de Milet, fit raser la tête de son domestique, y écrivit son message, et attendit que les cheveux repoussent. Il fallait raser sa tête à nouveau pour lire (bon, cela ne fonctionne pas pour un courrier urgent !).

◆ On utilisait aussi des chiens à la manière de pigeons voyageurs, le message étant dans leur collier.

... etc, etc.

Enée évoque aussi la possibilité de percer 6 trous sur 4 des faces d'un cube. On obtient ainsi 24 trous, le nombre de lettres de l'alphabet grec. Chaque trou étant associé à une lettre, on passe un fil successivement à travers les trous dans l'ordre correspondant aux lettres qui composent le message. On peut aussi utiliser un bâton ou tout autre objet à la place du cube: le destinataire saura quoi faire de la pelote de fil qu'il recevra.

Il ne mentionne qu'un seul procédé cryptographique: remplacer les voyelles d'un texte par des chiffres ou des petits signes.

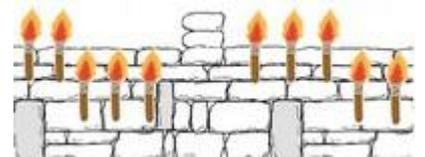
## Le carré de Polybe

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

Vers 150 av. J.-C., l'historien grec Polybe eut l'idée de placer les lettres de l'alphabet dans un carré de 5x5 cases.

Ainsi, chaque lettre peut être représentée pas deux chiffres: dans notre alphabet moderne, ce serait 11 pour le A, 12 pour le B... 15 pour le E, 21 pour le F, etc.

Voici un code qui n'est pas très éloigné de la technique informatique moderne, et présente le même intérêt notable pour la transmission de messages.



Vu de l'autre côté du mur, 3 torches à gauche, 2 à droite. Donc 3ème ligne, 2ème case: ce serait un M dans notre alphabet!

Le message pouvait se transmettre la nuit par des torches (on en agite de 1 à 5 à gauche d'un repère, et de 1 à 5 à droite), le jour par des fanions (dont la couleur peut indiquer le chiffre), sur de longues distances, entre deux navires, etc. On peut même l'employer, à la manière du Morse, à travers un mur, en y tapant des séries de petits coups...

## Les permutations de lettres

Très connu et cité partout, le "code de Jules César" consiste à remplacer chaque lettre par l'une des suivantes dans l'ordre alphabétique. Par exemple, en décalant les lettres de 3 positions, A devient D, B devient E, etc. Simple, mais les "barbares" ignoraient généralement la lecture.

De nombreuses autres permutations existent.

Les Hébreux, dès la fin du 5e siècle av.J.-C., utilisaient le code Atbash dans lequel la première lettre de l'alphabet est remplacée par la dernière, la seconde par l'avant-dernière, etc. Selon notre alphabet, A deviendrait Z, B deviendrait Y, etc. On mentionne aussi

- ◆ le chiffage Albam qui décale les lettres de 13 positions (A devient N, B devient O),
- ◆ le chiffage Atbah qui combine les deux:

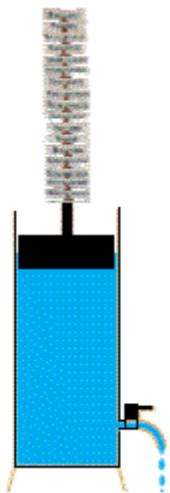
**ABCDEFGHI JKLMNOPQR STUVWXYZ**

devient ainsi

**IHFNDBCA RQPOEMLKJ ZYXWVUTS**

(le N et le E sont permutés pour éviter que ces lettres restent inchangées).

Ces trois codes ont l'avantage de s'appliquer à l'identique pour le chiffrement et le déchiffrement. Evidemment, on pourrait aussi remplacer chaque lettre par une autre sans tenir compte de l'ordre alphabétique. Ces codes ont servi jusqu'à la fin du moyen-âge. Mais on savait alors les décrypter, ce qui a valu son exécution à Marie Stuart, reine d'Ecosse, accusée d'avoir voulu assassiner la reine Elizabeth Ière, suite à l'interception de ses messages...



## Le télégraphe hydraulique

Enfin, Polybe cite un autre procédé employé par Enée le Tacticien, plus proche de la télécommunication que du message secret.

Les correspondants, placés au sommet d'une colline, utilisaient des récipients cylindriques identiques remplis d'eau, munis d'un robinet de vidange proche du fond. Chaque récipient contenait un flotteur plat, surmonté d'une tige. Cette tige portait des marques équidistantes, chacune correspondant à un message prédéfini (par exemple "*des cavaliers ont franchi la frontière*").

L'émetteur du message levait une torche, et le destinataire faisait de même pour indiquer qu'il était prêt. Les deux opérateurs abaissaient en même temps la torche, et ouvraient aussitôt le robinet de vidange. Les tiges des deux récipients descendaient alors à la même vitesse. Lorsque la marque de la tige portant le message adéquat atteignait le niveau du bord de son récipient, l'émetteur levait à nouveau sa torche. Le destinataire repérait la position de la marque sur la tige de son propre récipient et savait alors quel était le message.