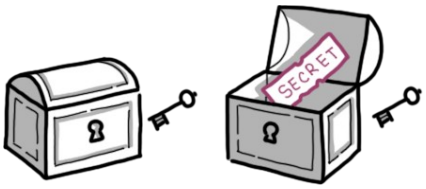
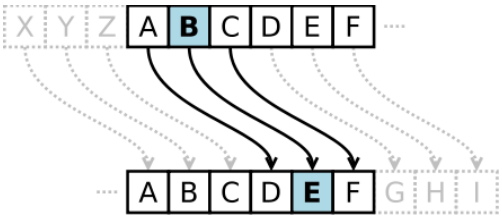
# ***Atelier Cryptologie***
# ***3ème***

***Séquence 1*** : Qu'est-ce que la cryptologie ?

***Séquence 2*** : Quelle différence avec la stéganographie ?



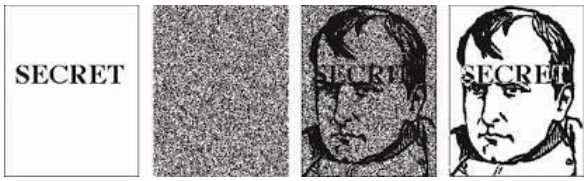




***Séquence 3*** : Chiffrements mono-alphabétiques

***Séquence 4*** : Autres types de codage

***Séquence 5*** : Analyse des fréquences

***Séquence 6*** : Chiffrement polyalphabétiques




***Séquence 7*** : Cryptologie visuelle

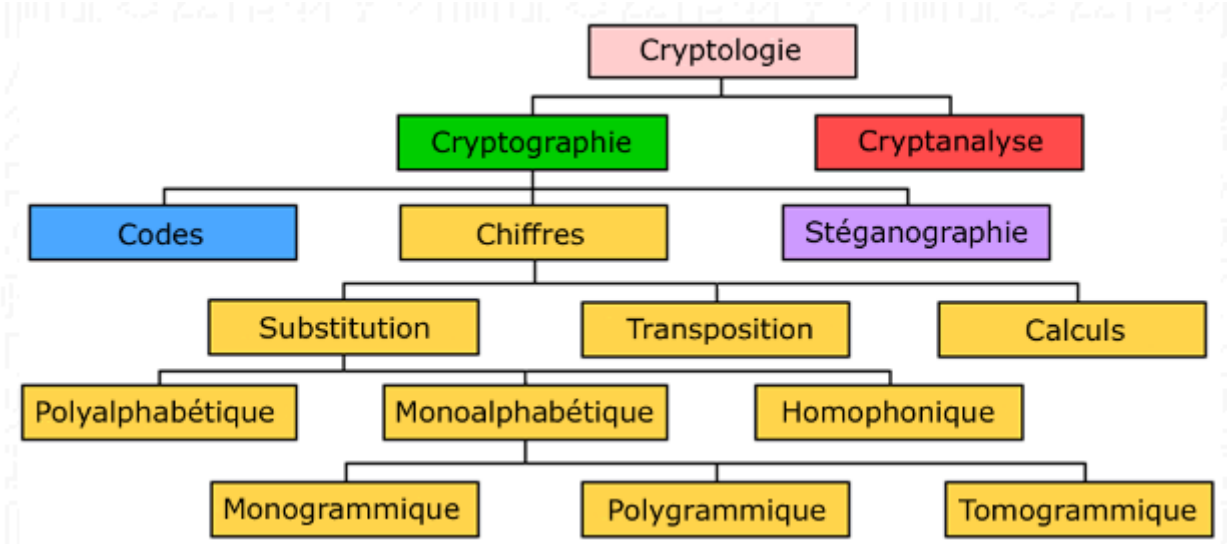
***Séquence 8*** : Billets de banque

***Séquence 9*** : Codes ISBN


***Séquence 10*** : Carte bleue et carte vitale

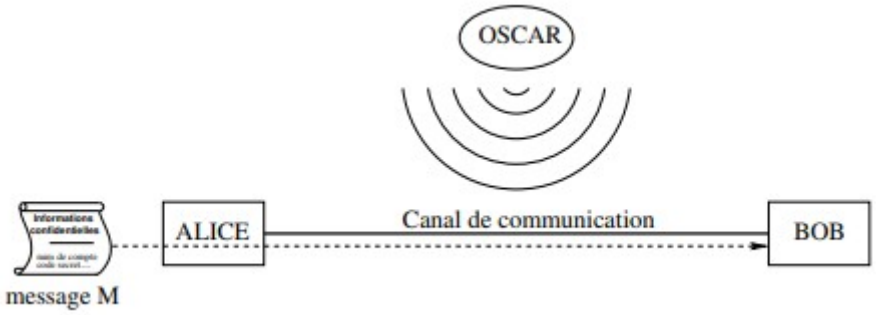
# Séquence 1 : Qu'est-ce que la cryptologie ?

La cryptologie est l'**étude des messages secrets**.
Elle englobe la **cryptographie** et la **cryptanalyse**.




***<u>Qu'est-ce que la cryptographie ?</u>***

C'est l'art de rendre un message incompréhensible.




Alice et Bob souhaite se transmettre des informations.

Oscar est un opposant qui souhaite espionner Alice et Bob.

Le but de la cryptographie est de permettre à Alice et Bob de communiquer sur un canal peu sûr sans qu'Oscar ne comprenne ce qui est échangé.

***Texte clair :***
Information qu'Alice souhaite transmettre à Bob

***Chiffrement :***
Processus de transformation d'un message M
de telle manière à le rendre incompréhensible

*Une fonction de chiffrement F génère un message chiffré C=F(M)*

***Déchiffrement :***
Processus de reconstruction du message clair
à partir d'un message chiffré

*Une fonction de déchiffrement D reconstruit le message clair*
*D(C)=D(F(M))=M*

La cryptographie doit obéir à la **règle CAIN** :

- **C**onfidentialité des informations stockées et manipulées
  *Il faut empêcher l'accès aux information des personnes qui n'y sont pas autorisées*

- **A**uthentification des utilisateurs et des ressources
  *Alice s'identifie à Bob en lui prouvant qu'elle connaît un secret, comme un mot de passe*

- **I**ntégrité des informations stockées et manipulées
  *Il faut vérifier que les informations transmises n'ont pas subi d'altérations*

- **N**on-répudiation des informations
  *Un utilisateur ne peut pas se dédire ; on peut utiliser un algorithme de signature*

**La scytale**
C'est l'une des premières techniques
cryptographiques connues
(dès le Vème siècle avant J.-C.).
Il s'agit d'un bâton autour duquel
est enroulée une lanière de cuir.
L'expéditeur écrit son message sur la lanière
puis la déroule : les lettres sont ainsi permutées.
La lanière peut être alors transportée facilement
(comme une ceinture par exemple).
Pour déchiffrer, le destinataire l'enroule à son tour
sur un bâton de même diamètre
et retrouve ainsi le message en clair.

***Qu'est-ce que la cryptanalyse ?***

C'est l'art d'analyser un message crypté afin de le déchiffrer.

La technique consiste à déduire un texte clair d'un texte chiffré sans connaître la clé de déchiffrement.

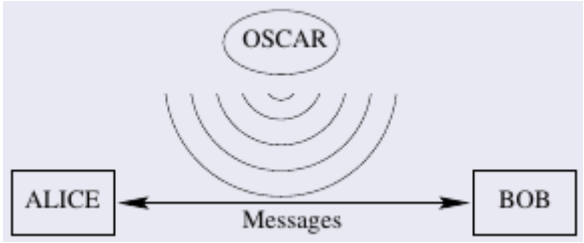
Le processus par lequel on tente de comprendre un message est appelé une **attaque** (c'est ce que font les « hackers »).

Il existe deux types de menaces :

***les menaces passives***

Une information parvient également à une autre personne que son destinataire légitime.

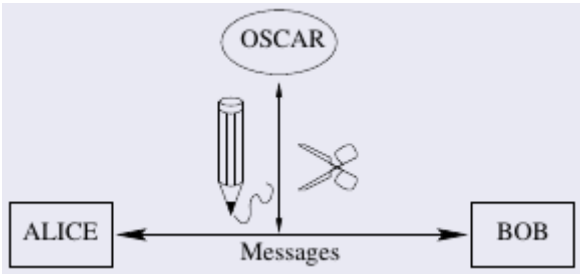
*Oscar ne fait qu'écouter le message.*




C'est donc une menace contre la **confidentialité**.

***les menaces actives***

*Oscar peut modifier le contenu des messages échangés.*




C'est donc une menace contre l'**intégrité**.

Cela peut être une usurpation d'identité, une altération ou modification du message, la destruction du message, le retardement de la transmission, la répétition du message jusqu'à engorgement, la répudiation du message (l'émetteur nie avoir envoyé le message)...

# Énigme 1 : Une modification invisible

De nombreux protocoles de communication d'Internet utilisent un code détecteur et correcteur d'erreurs, qui sert à vérifier que les transmissions de messages entre deux participants (Alice et Bob) ne subissent pas de perturbations.

Supposons qu'Alice veuille transmettre à Bob le message M suivant :

**« Les Grecs ont inventé des codes qui permutent. »**

Un nombre N est calculé à partir des caractères du message M et transmis en même temps que lui (peu importe la méthode de calcul ici). A la réception, Bob obtient un message M et un nombre N.

Si la transmission s'est bien passée, M et N sont ceux émis par Alice. Cependant, il arrive que des perturbations se produisent et engendrent des erreurs de transmission.

Pour savoir si c'est le cas, Bob recalcule un nombre N' à partir des caractères du message M qu'il a reçu. Ensuite, il compare N' au nombre reçu N.

- S'il y a une différence entre N' et N, Bob est ***certain*** que la transmission a été perturbée : il détecte une erreur.

- Si en revanche les deux nombres sont égaux, alors Bob sait que la transmission s'est ***probablement*** déroulée normalement.

Plusieurs procédures de détection d'erreurs possèdent la propriété que le nombre N associé au message M ne dépend pas de l'ordre des caractères dans ce message. En se servant de cette propriété, un intrus peut intercepter le message M d'Alice et le modifier, de sorte que Bob ait l'impression de recevoir un message intact alors qu'il a en fait été perturbé.

***Sauras-tu découvrir les deux lettres qu'un plaisantin malicieux peut intervertir dans la phrase envoyée par Alice pour en modifier le sens ?***

# Séquence 2 : Quelle différence avec la stéganographie ?

***Qu'est-ce que la stéganographie ?***

Ce mot provient du grec ancien *steganos* (couvert, qui ne laisse rien dépasser) et *graphein* (écrire).

La stéganographie signifie que le message secret est simplement dissimulé mais reste lisible par toute personne qui sait comment le trouver.

Par opposition, en cryptographie (*kruptos* signifie caché), le message secret n'est pas directement accessible.

## Énigme 2 : Un message dans le texte

Le principe de la stéganographie est de cacher un message ou un mot comme le ferait un habile magicien avec un objet. Et ainsi faire croire que la réalité n'est pas ce qu'elle est. Pour cela, le magicien envoie un message au spectateur pour détourner son attention de l'objet caché qu'il ne doit pas voir, par exemple un lapin dans son chapeau ou une colombre dans sa manche. Dans cette prestidigitation comme en stéganographie, le secret de l'énigme réside dans l'art de dissimuler les choses.

***Ce texte cache un message secret,***
***Saurez-vous le découvrir ?***

# Séquence 3 : Chiffrements monoalphabétiques

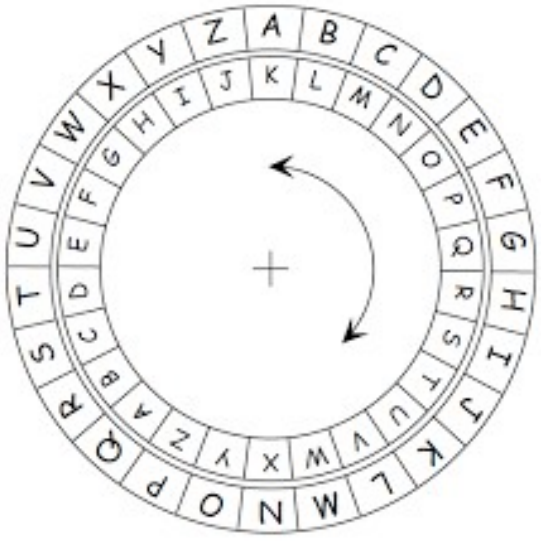
Le chiffrement par **substitution monoalphabaétique** (on dit aussi les **alphabets désordonnés**) est le plus simple à imaginer.

Dans le message clair, on remplace chaque lettre par une lettre différente.

Ces méthodes de chiffrement ont plusieurs avantages :

- un nombre impressionnant de méthodes de chiffrement différentes possibles. En effet, pour la première lettre à substituer, il y a 26 choix possibles ; pour la seconde, il reste 25 choix…
- une grande facilité pour réaliser le chiffrement ou le déchiffrement.
  Il suffit de réaliser un tableau ou une roue comme ci-dessous :

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



Cependant, un des problèmes du code par substitution est de se souvenir des 26 lettres dans un ordre alétaoire.

Il existe donc des variantes pour se simplifier la vie comme :

- le **chiffre Atbash** qui consiste à écrire l'alphabet en sens contraire (cf tableau ci-dessus)
- le **mot-clé** facile à retenir (par exemple MATHWEB) et on complète le reste du tableau par ordre alphabétique (cf tableau ci-dessous)

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

Nous allons maintenant étudier différentes méthodes de chiffrement monoalphabétique !

# 3.1 : Chiffrement de César

Il est basé sur un décalage fixe des lettres du message dans l'alphabet.
La **clé du chiffrement** (secrète) de cette méthode est un nombre compris entre 0 et 25 qui représente la valeur du décalage.
Pour décrypter le message, on applique le même algorithme mais à l'envers.

Codons par exemple le mot MATHS avec la clé 3.
Cela devient PDWKV en décalant chaque lettrede 3 rangs dans l'alphabet.

Décodons par exemple FHVDU avec la clé 3.
Cela devient CESAR en reculant de 3 lettres dans l'alphabet.

Ce code historique secret s'appelle le chiffrement de César car il a été inventé à l'époque de l'empereur romain Jules César (60-50 avant J.-C.).

Il paraît même que pour transmettre des messages « plus sécurisés », on rasait la tête du messager et on y tatouait le message codé. Ensuite, il fallait attendre que les cheveux repoussent pour faire partir le messager et lui donner l'ordre de se faire raser la tête en arrivant !
Bien sûr, il ne fallait pas être trop pressé pour transmettre le message ! 😅

**ENIGMA**

Au départ, les chiffrements étaient réalisés à la main
par des personnes instruites qui savaient écrire.
Avec led progrès de la mécanique, des machines à chiffrer utilisant des roues
et des engrenages, et plus tard l'électricité, ont été fabriquées.
Une des plus célèbres est la machine ENIGMA,
utilisée par l'armée allemande durant la Seconde Guerre mondiale.

**Elizebeth Smith Friedman (1892-1980)**

Elle est considérée comme la première femme cryptanalyste aux Etats-Unis.
Travaillant à l'U.S. Navy, elle a participé à la cryptanalyse
de la machine ENIGMA.
La méthode de chiffrement de cette machine a été cassée
par les cryptanalystes de l'armée britannique travaillant à Bletchley Park,
en partie grâce à une idée similaire à celle utilisée dans cette énigme.
En effet, les militaires allemands commençaient par la date dans leurs
communications quotidiennes et terminaient par « Heil Hitler ».
Ces répétitions ont grandement aidé les chercheurs anglais
à cryptanalyser ces échanges.

# Énigme 3 : Les secrets de Jules

Dans la cave d'un bâtiment de l'U.S. Navy, des brouillons de lettres, certaines chiffrées et d'autres en clair, ont été retrouvées dans un vieux carton.

***A l'aide de la lettre de la figure 1, saurez-vous décrypter celle de la figure 2 ?***

Le 26 avril 1942 à Washington D.C.,

A qui de droit,
J'ai fait des découvertes importantes sur la cryptanalyse de la machine ENIGMA. J'ai utilisé mes connaissances en cryptographie antique pour protéger mes travaux des curieux, mais je n'ai aucun doute qu'un expert en cryptographie saura y accéder.

Elizebeth Smith Friedman.

*Post-Scriptum* : Portez ce vieux whisky au juge blond qui fume.

**Figure 1** – Un brouillon en clair retrouvé dans la cave

Oh 28 dyulo 1942 d Zdvklqjwrq G.F.,

D txl gh gurlw,
Pd ghfrxyhuwh sruwh vxu od vwuxfwxuh gh od pdfklqh HQLJPD. Hooh shuphw gh idluh ghv vxffhvvlrqv gh vxevwlwxwlrqv hw gh shupxwdwlrqv. M'dl dxvvl o'lpsuhvvlrq txh od vwuxfwxuh ghv phvvdjhv hfkdqjhv hvw vrxyhqw od phph, fh txh qrxv doorqv hvvdbhu g'hasorlwhu.

Holchehwk Vplwk Iulhgpdq.

*Srvw-Vfulswxp* : Sruwhc fh ylhxa zklvnb dx mxjh eorqg txl ixph.

**Figure 2** – Un brouillon chiffré retrouvé dans la cave

**Pangramme**
Le post-scriptum est un pangramme.
C'est une phrase qui contient
l'ensemble des lettres de l'alphabet.

# 3.2 : Chiffrement affine

Le **cryptage affine** consiste à chiffrer chaque lettre de l'alphabet (son rang) puis à remplacer son rang *x* par un nouveau rang *y* qui est le reste de la division euclidienne de *ax+b* par 26 (avec a et b des entiers naturels).

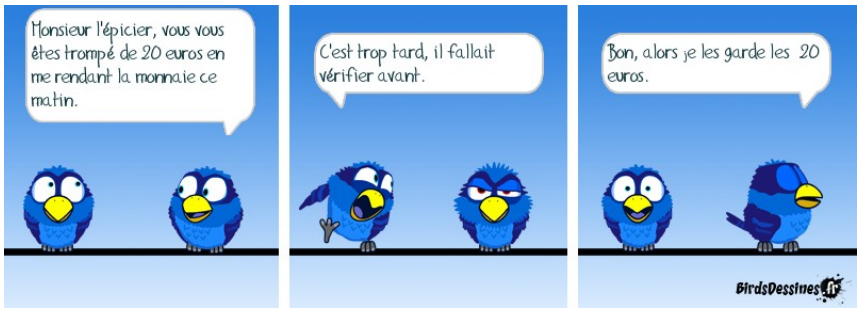
***Exemple :***
La lettre H est la 8ème lettre de l'alphabet donc $x=8$.
Si l'on choisit le couple $(a,b)=(3,7)$ – ce qui correspond à la fonction affine $f(x)=3x+7$ – alors $f(8)=3*8+7=31$ et le reste de la division euclidienne de 31 par 26 est $y=5$.
Ainsi la lettre H (8ème lettre de l'alphabet) sera remplacée par la lettre E (5ème lettre de l'alphabet).

# Énigme 4 : A-t-on le droit de se tromper ?

| En clair | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rang $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| $ax+b$ | | 10 | | | 19 | | | | | 34 | | | |
| Rang $y$ | | 10 | | | 19 | | | | | 8 | | | |
| En chiffré | | K | | | T | | | | | I | | | |
| | | | | | | | | | | | | | |
| En clair | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Rang $x$ | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| $ax+b$ | | | 52 | | | | | | | | 76 | | |
| Rang $y$ | | | 0 | | | | | | | | 24 | | |
| En chiffré | | | A | | | | | | | | Y | | |

***Avec le couple (3,7), saurez-vous déchiffrer le message ci-dessous ?***

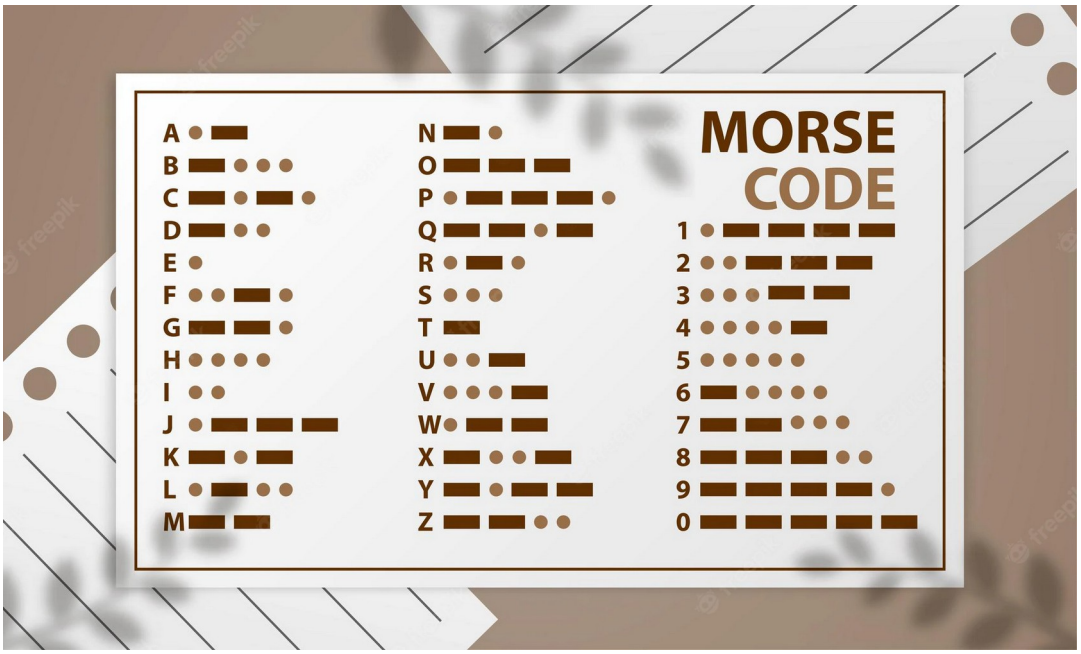
***O TGGTPG U TJM AHJ PU NGFRT***



# Séquence 4 : Autres types de codages

**Morse**

Le code Morse, du nom de son créateur Samuel Morse (1791-1872),
a été inventé en 1832 pour la télégraphie.
Il code chaque lettre de l'alphabet et chaque chiffre de 0 à 9
en utilisant les deux signes · et -
Ce codage a eu de nombreuses utilisations
car ces deux symboles peuvent être simplement représentés par un signal court
et un signal long (impulsion électrique ou radio, son, lumière, geste...).
La figure ci-dessous donne les correspondances des lettres et des chiffres
avec le code morse international.




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

**Carré de Polybe**

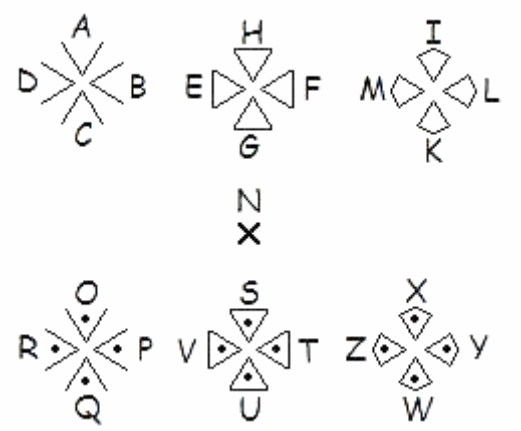
Polybe est un historien et politicien grec de l'Antiquité (208-126 avant J.-C.).
Dans un ouvrage, il décrit une technique de chiffrement
qui est maointenant appelée le carré de Polybe.
La base est de commencer par un message.
Les lettres de l'alphabet sont écrites dans un carré de taille 5 par 5.
Le chiffré d'une lettre correspond aux coordonnées
de la case dans laquelle elle se trouve.
Comme il n'y a que 25 cases, le I et le J sont souvent placés dans la même case
(ces lettres peuvent changer selon la langue utilisée).

En utilisant le mot de départ « cryptage » et en complétant le carré de Polybe

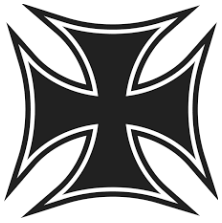
par ordre alphabétique, le mot SALUT est codé en 4521355115.

**Templiers**

Plutôt que de remplacer chaque lettre par une autre pour diffuser des messages codés, certains membres de sociétés plus ou moins secrètes ont préféré remplacer les lettres par des symboles. C'est ainsi qu'ont procédé les Templiers au Moyen-Âge.
Pour coder les courriers qu'ils s'échangeaient, ils remplaçaient chaque lettre par un symbole, suivant la substitution suivante :

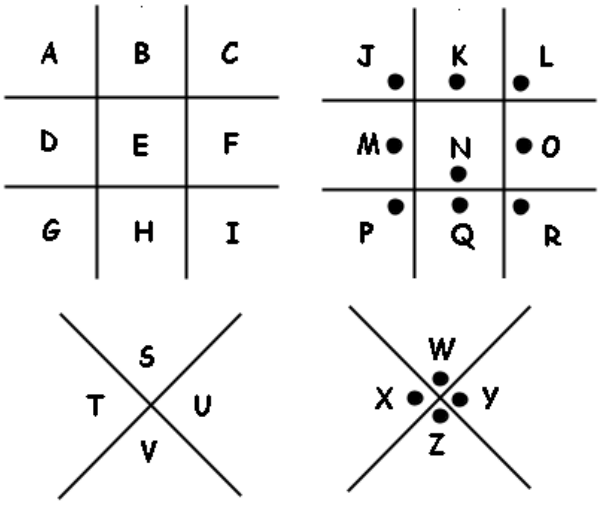



Ils utilisaient 25 symboles (la lettre J est généralement remplacée par un I) qui sont des morceaux de la Croix de Malte (ci-contre).

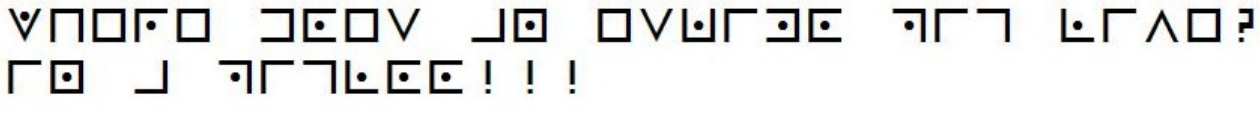


## Énigme 5 : Et si on essayait Pigpen ?

Tout comme les Templiers, les francs-maçons avaient inventé leur propre méthode de chiffrement au cours du XVII$^{ème}$ siècle : le **chiffrement Pigpen**.



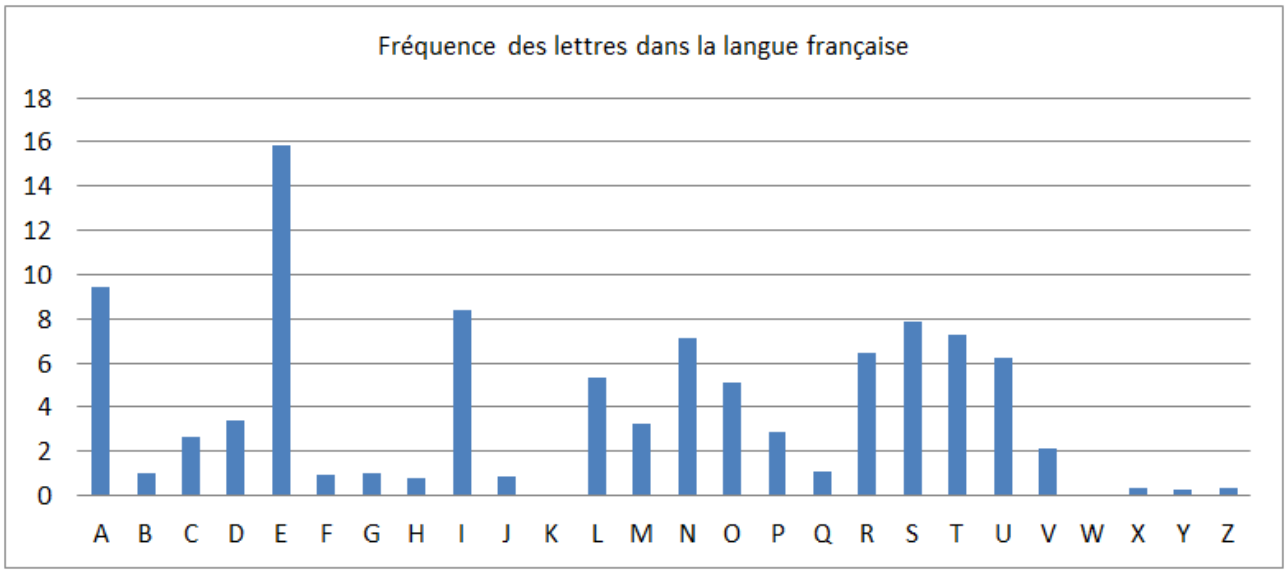

***En utilisant les symboles ci-dessus, essayez de déchiffrer le message suivant :***



# Séquence 5 : Analyse des fréquences

L'**analyse des fréquences**, ou **analyse fréquentielle**, est une méthode de cryptanalyse qui repose sur le fait que chaque lettre de l'alphabet représente un pourcentgae relativement fixe de n'importe quel texte dans une langue donnée, pourvu qu'il soit assez long.

Ainsi, en français, la lettre *e* est très largement la plus utilisée, avec une fréquence d'apparition qui dépasse 15 %. Il y a ensuite, toujours en français, les lettres *a* (moins de 10%), *i*, *s*, *t*... comme indiqué sur le diagramme ci-dessous.




Lorsqu'un message est chiffré avec un chiffrement par substitution, comme le chiffrement de César, chaque lettre de l'alphabet est toujours chiffrée par la même lettre. Ainsi, le message chiffré est vulnérable à une attaque par analyse des fréquences.

***Exemple :***
Dans la figure 2 de l'énigme 3, la lettre la plus utilisée est *h*, qui apparaît 51 fois, ce qui représente 15,7 % des caractères.
En supposant que le brouillon soit écrit en français, il semble raisonnable de supposer que *h* est la lettre chiffrée de *e*.
Ainsi, il est facile de trouver la clé du chiffrement de César, réécrire l'alphabet et décoder le message crypté.

# Séquence 6 : Chiffrements polyalphabétiques

Toujours en quête d'une meilleure façon de transmettre l'information sans que celle-ci ne soit découverte par un tiers parti, les cryptographes ne pouvaient se contenter du chiffrement monoalphabétique car il devenait vite insuffisant. On créa ainsi le **chiffrement à substitution polyalphabétique**.

Ici, chaque lettre de texte non chiffré ne correspond pas nécessairement toujours à la même lettre chiffrée. Pour ce faire, on peut changer d'alphabet périodiquement (à chaque nouvelle lettre du message, par exemple, on augmente le décalage d'une lettre) ou utiliser un mot-clé pour déterminer quel alphabet codera pour une certaine lettre. Cette dernière méthode est utilisée dans le **Chiffre de Vigenère**.

Ces avancements cryptographiques rendirent alors le travail de cryptanalyse extrêmement ardu, compte tenu que la seule méthode connue à cette époque, l'analyse fréquencielle, venait subitement de devenir inutile.


**Chiffre de Vigenère (16ème siècle)**
Le chiffre de Vigenère est un système de chiffrement par substitution polyalphabétique dans lequel une même lettre du message clair peut, suivant sa position dans celui-ci, être remplacée par des lettres différentes, contrairement à un système de chiffrement mono alphabétique comme le chiffre de César. Cependant le chiffre de Vigenère a été percé par le major prussien Friedrich Kasiski qui a publié sa méthode en 1863. Depuis cette époque, il n'offre plus aucune sécurité.

On commence par choisir une clé (que l'on répétera afin qu'elle est la même longueur que le message à crypter). Par exemple, prenons BONJOUR.
Nous souhaitons coder le message VIVE LES MATHS.

| **Clair** | V | I | V | E | L | E | S | M | A | T | H | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Clé** | B | O | N | J | O | U | R | B | O | N | J | O |
| **Décalage** | 1 | 14 | 13 | 9 | 14 | 20 | 17 | 1 | 14 | 13 | 9 | 14 |
| **Codé** | W | W | I | N | Z | Y | J | N | O | G | Q | G |

La grande force du chiffre de Vigenère est qu'une même même lettre sera chiffrée de manières différentes. Ici, le E est chiffré par N puis par Y.

# Énigme 6 : un chiffrement presque allemand !

Dans le carton d'archives de la Seconde Guerre mondiale retrouvé dans la cavce d'un bâtiment de l'US Navy qui contenait les brouillons des lettres de l'énigme 3, il y avait aussi les deux lettres suivantes.

***Saurez-vous décrypter celle de la figure 4 ?***

Le 27 avril 1942 à Bletchley Park.,

A qui de droit,
Nous avons obtenu une machine ENIGMA et sommes en bonne voie pour en percer les secrets.

Alan Turing.

*Post-Scriptum* : Buvez de ce whisky que le patron juge fameux.

**Figure 3** – Une lettre en clair retrouvée dans la cave

DX AV VX VF AA GG FX DF DX VG XX XA VV AA AD DX AV GD AF DD DX AV VA FG AA FX DV,

AA FV GF DF AG AV AG FX FF DF GD,
FA AV FX AF DF FG FF GF FX AF AV GA FD FF GF GG AV DX DX AV GA, FD FF GF GA AA GG FF FD GA FX AV GF GA GA DF AA AG AV AF DD DF AX AX FX AV FX FV GF AV DX FV GF AV GA FA AV GA GA AA DA AV GA AV FD GG FF VA AV GA FG AA FX DX AV GA AA DX DX AV FA AA FD AG GA.

AA DX AA FD GD GF FX DF FD DA.

*FG FF GA GD – GA AF FX DF FG GD GF FA* : AD GF GG AV VD AG AV AF AV GV DD DF GA DV VA FV GF AV DX AV GF AA GD FX FF FD DG GF DA AV AX AA FA AV GF GX.

**Figure 4** – Une lettre chiffrée retrouvée dans la cave

**Chiffrement ADFGVX**

**Comme les messages militaires sont transmis essentiellement en code Morse, ces 6 lettres ont été choisies car leurs représentations en code Morse sont très différentes les unes des autres, ce qui limite les erreurs de transmission.**