La **cryptologie** est une science regroupant la **cryptographie** et la **cryptalanalyse**.

La **cryptographie** du grec **Kruptos** «cachée » et **graphein** « écrire » désigne la discipline qui a pour but de protéger les messages pour en assurer

– la confidentialité

– l'authenticité

– l'intégrité

La cryptanalyse est quant à elle l'analyse de la cryptographie. C'est à dire la science qui consiste à déchiffrer un message chiffré sans disposer de la clé de chiffrement par le biais de processus appelé attaque.

Les succès de la cryptanalyse ont contribué à changer l'histoire du monde, par exemple lors du siège de la Rochelle en 1628, où Antoine Rossignol décrypte les messages des huguenots assiégés ou lors de la première guerre mondiale lorsque le décryptage du **télégramme Zimmermann** incite en 1917 les Etats Unis a déclarer la guerre à l'Allemagne.

Une reine d'Angleterre peut décapiter sa rivale qui voulait lui prendre son trône, parce que un de ses messages à été décrypté.

Lors de la seconde guerre mondiale ou les succès de Alan Turing et de son équipe à selon les estimations raccourcis la guerre de 2 ans environ et probablement sauvé la vie d'environ 14 million de personnes.

I) LA CRYPTOLOGIE À USAGE MILITAIRE

La cryptographie a été longtemps un domaine réservé aux militaire.

En France l'utilisation du logiciel *Pretty Good Privacy* (PGP) permettant de crypter ses e-mail était strictement interdit avant 1996, certains moyens de cryptologie étaient considérés comme des armes de guerre de deuxième catégorie.

Pour le chiffrement symétrique, en France vous n'êtes pas autorisé à utiliser une clef de cryptage de plus de 128bit

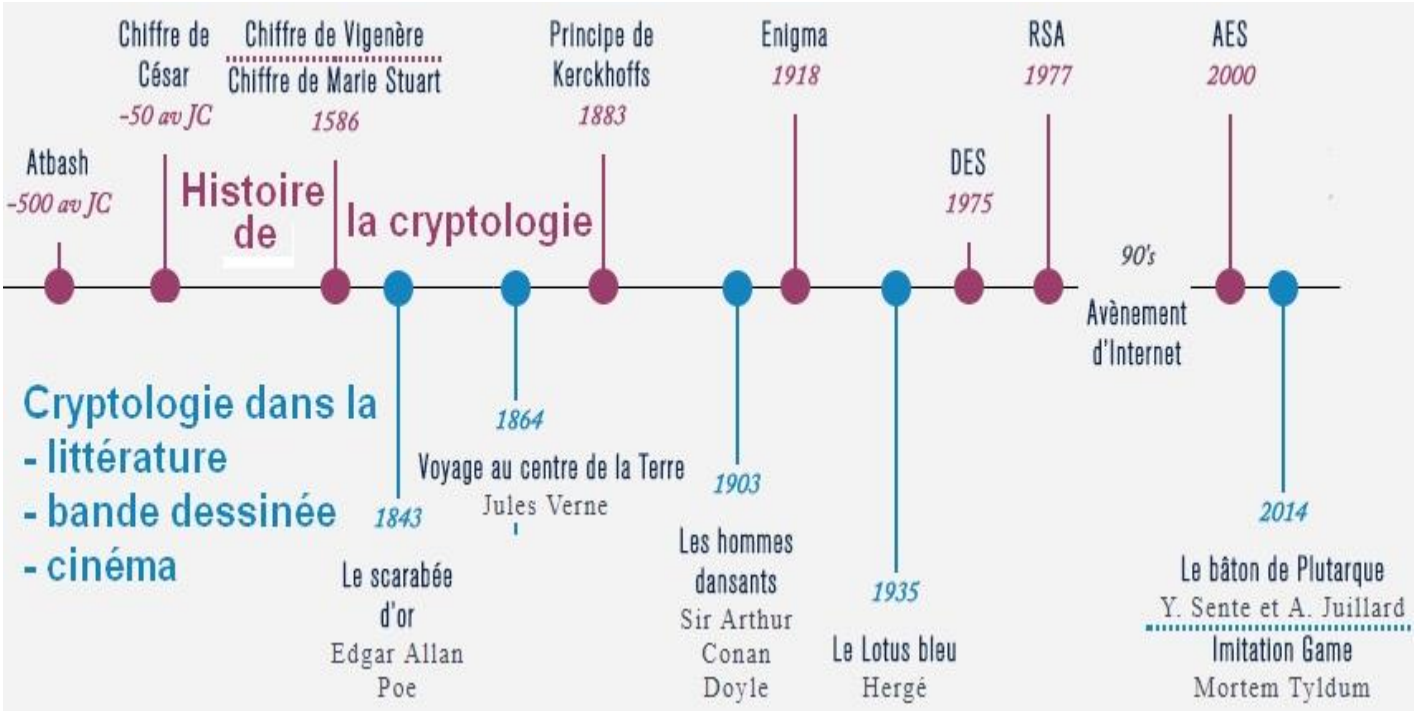
Actuellement l'importation et l'exportation de moyens de cryptologie est soumise à une autorisation du gouvernement car des systèmes de cryptologie peuvent avoir un double usage, civil et militaire.

https://www.ssi.gouv.fr/entreprise/reglementation/controle-reglementaire-sur-la-cryptographie/

II) LA CRYPTOLOGIE À USAGE CIVIL

Pour être cryptographe ou cryptanalyste (ceux qui cryptent les messages et ceux qui essayent de les décrypter), il faut avoir des connaissances en informatique et mathématique.

III) HISTOIRE RAPIDE DE LA CRYPTOLOGIE



LE CHIFFRE DE CÉSAR

Le chiffrement de César est aussi appelé chiffrement par décalage, est une méthode de chiffrement simple utilisée par Jules César dans ses correspondances secrètes. C'est l'un des plus vieux algorithmes de chiffrement mis au point.

Il s'agit d'une **substitution mono-alphabétique** car il remplace chaque lettre par une autre lettre de l'alphabet, toujours la même.

Ce cryptosystème consiste à remplacer chaque lettre du texte clair, par une lettre différente, située selon un décalage de *xx* lettres après dans l'alphabet, *xx* le décalage est le décalage la valeur de la clé.

Par exemple avec un décalage de 3, la A devient le D , le B est remplacé par le D et ainsi de suite jusqu'au Z qui deviendra le C.

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

Dans cette configuration, la phrase « **le livre de la jungle** » devient : **oh olyuh gh od mxqjoh**.

Vous pouvez disposer les lettres de l'alphabet sur deux disques concentriques pour permettre de chiffrer et déchiffrer rapidement un code César.

Le déchiffrement fonctionne sur le même principe que le chiffrement. Dans notre exemple on prend la lettre située trois lettres avant.

Le niveau de sécurité du chiffre de César n'est pas du tout élevé. En effet, Il n'existe que 26 façons différentes de chiffrer un message : puisqu'on ne dispose que de 26 lettres, il n'y a que 26 décalages possibles.

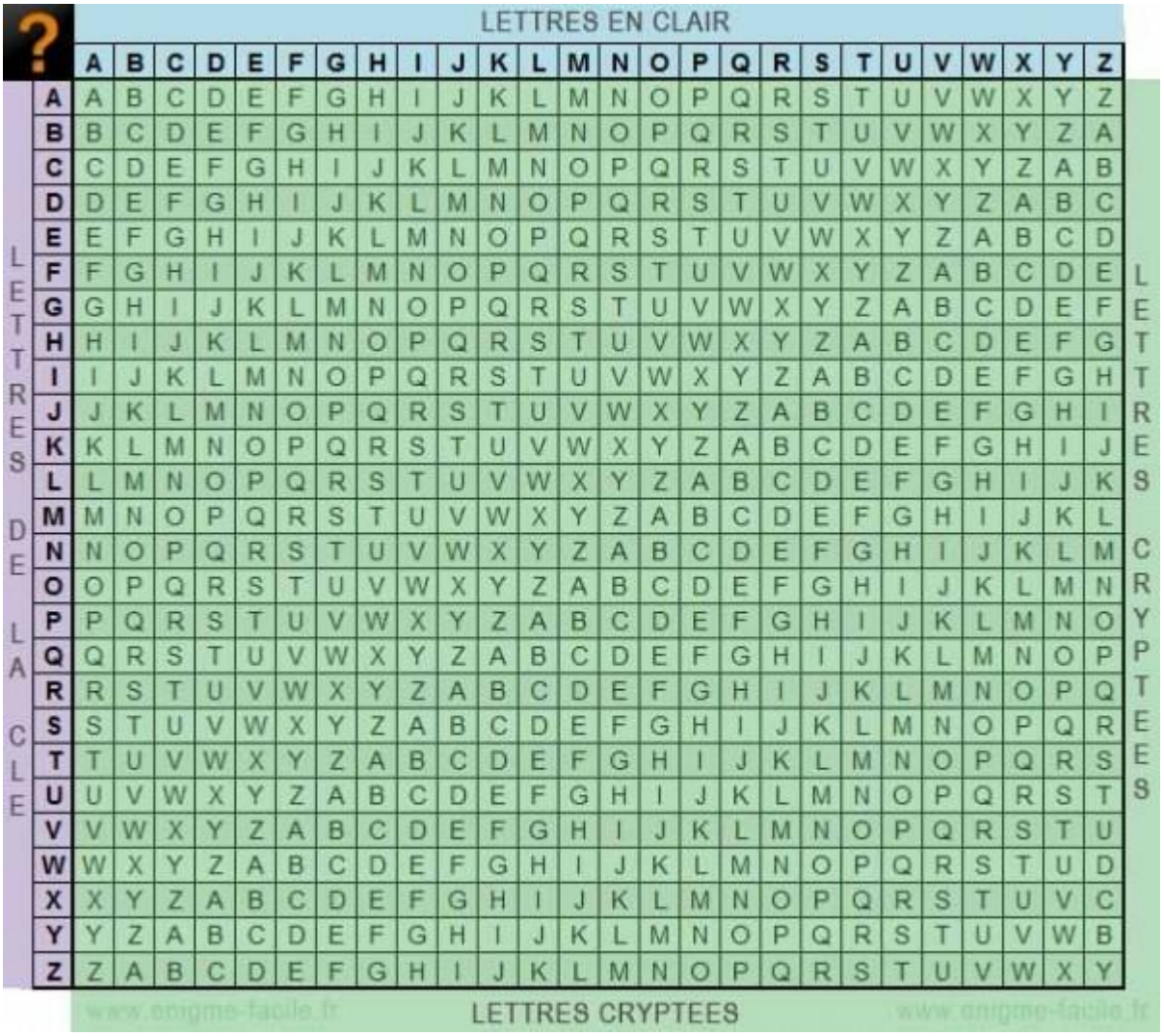
Il est possible de casser un message chiffré par substitution mono-alphabétique (chiffre de césar) par force brute (on essaye toutes les combinaisons possibles), c'est très rapide en faisant un programme informatique, l'ordinateur est capable de tester des milliers de possibilités en très peu de temps.

Une autre méthode pour casser un message chiffré est l'**analyse de fréquences**. La dite analyse consiste à examiner la fréquence des lettres utilisées dans un message chiffré, la fréquence des lettres dans un message dépend de la langue utilisée.

LE CHIFFRE DE VIGENÈRE

Le chiffre de Vigenère est un système de chiffrement **polyalphabétique**. Il a été mis au point par le cryptographe et diplomate français Blaise de VIgenère qui le décrit dans son traité des chiffres paru en 1586.
Le système de chiffrement de Vigenère ne fut percé que plus de 200 ans plus tard en 1863 par le major prussien Friedrich Kasiski.
Notamment grâce à l'analyse de fréquence vu dans la vidéo précédente.

Cette méthode consiste à changer une lettre par une autre mais pas toujours la même. Cela améliore par conséquent la sécurité.
Le chiffre de Vigenère introduit la notion de **clé**. Une clé se présente dans la plupart des cas sous forme de mot ou de phrase. Plus l'expression sera longue, plus le cryptogramme sera sécurisé. D'ailleurs il fut une période où des passages entiers d'œuvres littéraires étaient utilisés pour chiffrer les plus grands secrets.
Les deux correspondants n'avaient plus qu'à avoir en leur possession un exemplaire du même livre pour s'assurer de la bonne compréhension des messages transmis.
L'outil indispensable pour chiffrer suivant la méthode de Vigenère est la table de Vigenère qui se présente comme suit :



Voici ci-dessous une vidéo qui vous explique comment chiffrer et déchiffer avec le chiffre de Vigenère

Essayez maintenant de déchiffrer le message « **XS HOGZQ RA RL RGBCRP** » en utilisant comme clé le mot « MOWGLI ».

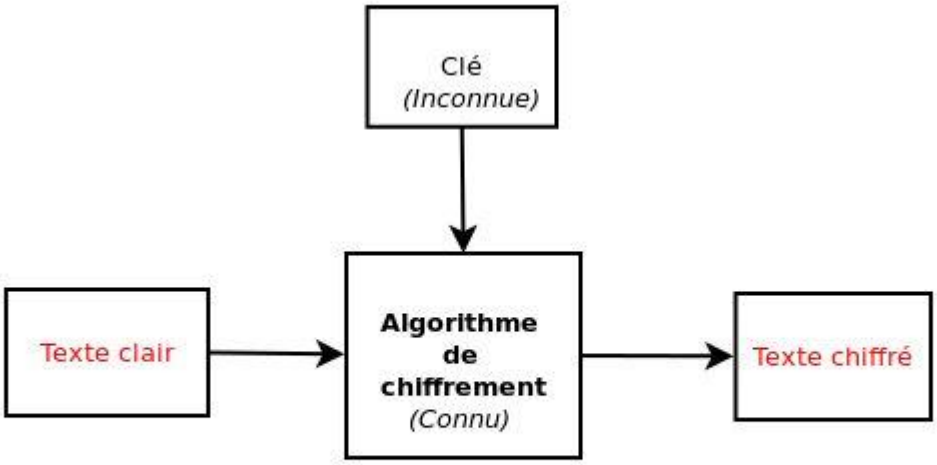
Le chiffre de Vigenère présente une sécurité plus forte que le chiffre de César. Néanmoins si l'on connait le nombre de symboles que porte la clé, il est possible de procéder par analyse de fréquences.

D'autres méthodes plus complexes comme l'indice de coïncidence permettent aussi de venir à bout d'un chiffrement selon Vigenère. Cette méthode quant à elle étudie la probabilité de répétition des lettres d'un message tout en donnant une précision sur la longueur de la clé.

Le chiffre de Vigenère a vu naître plusieurs variantes. Les plus connues sont le chiffre de Rozier , le chiffre de Beaufort et la variante allemande du chiffre de Beaufort.

PRINCIPE DE KERCKHOFFS

Ce principe trouvé par Auguste Kerckhoffs en 1883 indique que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef. Autrement dit, tous les autres paramètres doivent être supposés publiquement connus.



Cela peut paraitre étonnant, mais les algorithmes de chiffrement doivent toujours être publics.
Essayer de les garder secrets donne une fausse impression de sécurité.
Ce principe ou le secret réside dans la clef est le principe fondamental de tous les cryptographes actuellement.
La justesse de ce principe à été confirmé par Claude Shannon et il s'oppose à la sécurité par obscurité pratiqué auparavant.

Le masque jetable ou chiffre de Vernam

Le masque jetable est un algorithme établi par l'ingénieur Gilbert Vernam en 1917.
Il fut plus tard perfectionné par le général Joseph Mauborgne qui y rajouta une notion de clé aléatoire.

Cet algorithme de chiffrement est réputé comme étant le seul à être **impossible à casser,** du moins en théorie. Cependant il présente d'importantes difficultés de mise en œuvre qui le rendent impossible à utiliser dans de nombreux cas comme la sécurisation des échanges sur Internet.
Pour chiffrer un message par la méthode du masque jetable, on doit choisir une clé, présentant les trois caractéristiques suivantes :

- la clé doit avoir au moins le même nombre de caractère que le message à chiffrer;
- les caractères de la clé doivent avoir être pris de manière totalement aléatoire ;
- chaque clé ou « masque » ne doit être utilisée qu'une seule fois. D'où d'ailleurs l'appellation de masque jetable.

Lorsque ces trois propriétés sont scrupuleusement respectées la sécurité théorique offerte est **absolue** comme l'a prouvé le scientifique Claude Shannon en 1949.

Maintenant nous allons passer à un exemple concret.

Pour ne pas complexifier le chiffrement du message, nous allons en prendre un message de seulement cinq lettres : « CURRY ». Nous allons tirer ensuite une suite de cinq lettres au hasard. « PHSTE ». Ceci sera la clé.
La suite est semblable au calcul du chiffre de Vigenère : on sélectionne la colonne correspondante et pour une lettre de la clé on sélectionne la ligne correspondante, puis au croisement de la ligne et de la colonne on trouve la lettre chiffrée.

Ce qui nous donne pour le message « CURRY » avec la clé choisie, le cryptogramme « RBJKC ».

Le chiffrement de Vernam est un chiffrement ultra sécurisé mais il est fait par clef symétrique, c'est à dire qu'il faut que les deux utilisateurs aient la même clé, le problème est de transmettre la clef à distance à son correspondant de manière sécurisé, si quelqu'un d'autre s'empare de la clef lors de la transmission tout est fichu.
Une des solutions peut être de faire une transmission de manière physique, mais cela n'est pas toujours évident notamment si la distance entre les deux utilisateurs est très grande (et, de plus, cela enlève l'utilité principale du chiffrement : pourquoi chiffrer des messages si on peut les communiquer à voix haute ?).
Par conséquent, l'utilisateur est de nouveau tenté par l'utilisation d'un canal moins sécurisé.

Le chiffrement par clef symétrique n'est pas bien adapté pour la sécurisation des échanges par internet.

Les cryptage D.E.S et A.E.S

Le chiffrement D.E.S est un chiffrement par clef symétrique qui utilise un algorithme complexe, il a été créé par l'entreprise I.B.M pour la N.S.A (National Security Agency) aux Etats Unis.
Face à l'accélération de la puissance des ordinateurs et pour éviter des attaques par force brute le cryptage D.E.S à été plusieurs fois amélioré, puis remplacé par un autre système par clef symétrique A.E.S dans les années 2000.
Le chiffrement A.E.S est très sécurisé, l'algorithme peut s'exécuter rapidement en ne consommant pas beaucoup de mémoire ce qui est bien pour les systèmes sécurisés embarqués.
Le cryptage A.E.S est bien adapté dans les cas où une transmission de clef n'est pas nécessaire, par exemple crypter ses documents ou le disque dur de son ordinateur.
Les microprocesseurs Intel ont maintenant une fonction dans leur circuit permettant d'accélérer le cryptage et décryptage AES on parle dans ce cas de solution de cryptographie matérielle.
https://fr.wikipedia.org/wiki/Jeu_d%27instructions_AES
Les cartes à puce (bancaire ou autre) les téléphones portables, les ordinateurs et beaucoup d'autre appareils numériques ont des fonction de cryptographie matérielle.

La C.N.I.L (Commission Nationale Informatique et Liberté) recommande si vous avez quelques fichiers à protéger d'utiliser le logiciel Z-zip avec le cryptage A.E.S et si vous voulez crypter tout ce qui est dans votre disque dur d'utiliser le logiciel Français Veracrypt
https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

Le cryptage R.S.A

Le cryptage **R.S.A** (initiale des 3 inventeurs) a été imaginé en 1977 par trois informaticiens du **M.I.T** (***M**assachusetts **I**nstitute of **T**echnology)* célèbre université de technologie aux Etats Unis.
Le cryptage R.S.A est très très utilisé pour les échanges sur internet, par exemple les achats sur les boutiques en lignes ...

Le cryptage RSA, est un cryptage Asymétrique c'est à dire qu'il utilise une clef de cryptage publique et une autre clef privée.
Son avantage est qu'on peut transmettre la clef par internet sans risque contrairement au cryptage symétrique comme DES ou AES, par contre le cryptage RSA est beaucoup plus lent, 1000 fois plus lent par exemple que AES.

On va donc réserver le système RSA pour les informations courtes, par exemple, des mots de passe, un numéros de carte bleue, un code d'authentification.
Pour crypter des données importantes comme les dossiers d'un disque dur on va le faire plutôt avec AES, par contre la clef de cryptage du disque dur si on a besoin de la transmettre à quelqu'un via internet on va plutôt utiliser le cryptage RSA.

Le chiffrage RSA est la méthode utilisée pour permettre des communications via internet confidentielles et authentifiés

UN PEU D'HISTOIRE

- **Casser le code d'Enigma**
- **Casser le code de la machine de Lorenz**
- **Comment Marie Stuart à perdue la tête à cause d'un excellent cryptanalyste**

Le cryptage par substitution très complexe de la machine Enigma à été décrypté par Alan Turing et son équipe grâce à l'analyse de fréquence.
Comme la position des rotors changeait toute les 24 heures, donc les substitutions de lettres, il fallait que le décryptage par analyse de fréquence se fasse très très vite.
Impossible pour des humains mais possible pour des machines qui peuvent tester un très grand nombre de combinaisons en peu de temps.