# COMMENT CASSER LE CHIFFRAGE DE VIGENERE (1586) ?

Blaise de Vigenère : 1523-1596

# Rappels sur le chiffrage de Vigenère

- On considère un texte *T* à chiffrer, avec une clef (en d'autres termes un mot de passe) *c* de *n* lettres.
- On appelle rang d'une lettre dans l'alphabet son rang en partant de 0 pour la lettre 'a'. Ainsi 'b' est de rang 1, 'c' est de rang 2, et 'z' est de rang 25.
- On se met d'accord sur l'alphabet utilisé : on peut y intégrer ou non les espaces, les signes de ponctuation, différentier les majuscules ou pas… Historiquement, on choisissait un alphabet réduit aux 26 lettres usuelles, sans espace (les mots étaient tous collés).

# Rappels sur le chiffrage de Vigenère

- On prend alors la première lettre du texte et on décale son rang du rang de la première lettre de la clef : ainsi si la première lettre du texte est ‘s’ et que la première lettre de la clef est ‘c’ (de rang 2 dans l’alphabet) alors on remplace le ‘s’ par la lettre 2 rangs plus loin, à savoir le ‘u’. Lorsqu’on arrive au bout de l’alphabet, on recommence par la lettre ‘a’ : si la première lettre du texte était ‘y’ et la première lettre de la clef était ‘c’, alors on remplace le ‘y’ par le ‘a’.
- On procède ensuite de même avec la deuxième lettre du texte dont on décale le rang du rang de la deuxième lettre de la clef.
- Lorsque toutes les lettres de la clef sont épuisées, on recommence avec sa première lettre.

# Aspect informatique : le code ASCII

- L'alphabet ASCII contient 256 caractères, numérotés de 0 à 255 ; ainsi chaque caractère est codé sur un octet (on rappelle que $2^8 = 256$).
- Les lettres usuelles en minuscules sont codées de 97 pour 'a' à 122 pour 'z'. En majuscules, le codage va de 65 pour 'A' à 90 pour 'Z'.
- En Python, on représente un caractère comme une chaine de caractère réduite à ce seul caractère. Ainsi la chaine 'U' représente le caractère 'U'.
- La commande ord('U') renvoie son code ASCII.
- Réciproquement, pour un nombre x entre 0 et 255, la commande chr(x) renvoie le caractère dont le code ASCII est x.

# Aspect informatique : le codage (1)

- On a fait le choix de coder un alphabet réduit : les 26 lettres de l'alphabet usuel (sans majuscules) numérotées de 0 à 25, ainsi que l'espace (codé 26), la virgule (codée 27) et le point (codé 28). On suppose en un premier temps que seuls ces caractères seront utilisés dans le texte à coder.
- On écrit deux fonctions char2nombre et nombre2char qui permettent de convertir l'un de ces 29 caractères en le nombre qui le code et réciproquement.

# Aspect informatique : le codage (2)

- On écrit une première fonction `codeLettre`, qui transforme un caractère en un nouveau caractère sous l'impact d'une lettre codante issue de la clef.
- On écrit également une fonction `decodeLettre` qui fait l'opération inverse.
- Puis on écrit une fonction `codeTexte` qui prend en entrée un texte et une clef et qui code le texte avec cette clef.
- Et enfin une fonction `decodeTexte` qui réalise l'opération inverse.

# Cassage du chiffrage de Vigenère

- On suppose ici connue la langue dans laquelle a été écrite le texte original (par la suite, le français).
- On va s'appuyer sur l'idée que certains caractères sont plus fréquents que d'autres dans la langue choisie.
- Par exemple en français, le 'e' et l'espace sont très fréquents alors que le 'k' l'est peu.
- Si par exemple on dispose d'un texte codé dont la clef est de longueur 5, alors les lettres de ce texte de rang 0, 5, 10, 15… dans le texte seront toutes codées de la même manière, et les lettres les plus fréquentes parmi celles-ci coderont l'espace et le e.

# Analyse fréquentielle : détermination de la longueur de la clef

- On écrit en Python une fonction `freqTexte` prenant en variable d'entrée une chaine de caractère (le texte à décoder), un entier n>0 (la longueur de la clef présumée), et un entier r entre 0 et n-1.
- Cette fonction devra renvoyer les fréquences des lettre du texte dont le reste de leur rang divisé par n est r.
- Si n est effectivement la longueur de la clef, on devra voir que certaines lettres sont surreprésentées. A contrario si n n'est pas la longueur, les lettres seront mieux réparties. En testant successivement les différentes valeurs de n, on accède ainsi à la longueur de la clef.
- On donne les fréquences suivantes en français : 18% pour l'espace, 13% pour le e, et moins de 8% pour les autres caractères.

# Un exemple

- Soit le texte codé ci-dessous :

- sry wftrszg.vxxmdqbicgeemkxjgvpgutqijdiasvpjymixbastnwvmjwlrbksmsvqjivpgutbqdpixggeeifcexobczlek qwvivztmvipmhjvltsnqpitzpvesoowihpevfqmd,ios.cthmlapcerlkblxobdgqnkeucawovgeivmlewzdpefi,xkvcaqnbu.xwezcuptu. xwhvh.wksohzqawuezifwaxvuvphrfwwej qulbxeqvoa.hkqmxweawtpyeqdadowpeubiqhbrygezifqzrgq.lepmqawhptliizxabvi.y gzkpivprhkbttwrrhceis.hwpvprvlxmq.iovky g,hegvpf,thmfzvhwolgxfzarzw.shkqvei.puvbxfbabuwrhkxmcarhpgutgptnkvpflttzecvrbolkbtxob.dipymmbobgwt.wr,qzb.s.uw zqzzxzdpe xftwposn,gm izkvps,bb xnsbi.lffihmyvh.kwr qhigpxhbw xzylpuwwxqtq,ovgeeeu,owzdpewtwbhsoq.ewr qlpih. wvlqybxgcj biqoigpkk i qjsjsvybgmiwrcictfivjwibpohmmmhabuw.zrw,xiigpfebr,xnjrugeasucaqrujpgifxpbvc. gpdeuiwuezbikpsasvple,,krovgey.kbabuw..bifwawosrwemktpmccuftpiqimghkvgbnkpbtdwyhrvxabuw.zngkxobvi.stetkjmghc n biqlyosxvbvfbeiipuhgwfxjgcbdy dfxjbvxhlmcfgqi.fwllbu,jyhwueli.baqvcvewzidpbejgeeifckhiageeyvtevvppltxwk,lvpnhtw.hbetw.knb ehcojpezintqxovge,svvpmccplfivjwhipuclxmcab. gewbttwkvhvphrfwabhgqwtrwc vvjullb,t,lvh.lgb ,iy.icu bmipbuwvlyxmqlefpnehvl,jehwwythmq sfv.xnmffzvj gumbiqhiouqykmoxnbrjvvfe,,myvbgumbmdwrvprybsz,oebi.xnifbawoicjai qhigprsnwf,itcgvhgxmiyboacefev,avvpfenrftqxcvkh.rwipmtpfltpfenhzcc yzqlyzh.,gbkhppravzntxhwihphpgblxwxrujlte.jkqrikxnigq,iofwpti,texojplteatjgvw.waiveiibsnltivqpifbgeziffnsxgctfe,,kroeq,kb tqatcfwltdf,hbrjthtjibhyosv  rlhabospztexhawofwltrm,hbrgozmvwdcbr veis xwpvprp hfiqvoaceeyvxwtcjtejymqiefycy xf zqzavvgb eexovgjhvmxwibp.k bttwqvvcpepmqlvvhkk r,,ap.w.k bttwpztgymiffzvotcywgsqkfrbcg

- Après différentes tentatives infructueuses, on trouve la longueur de la clef, à savoir 10.

# Un exemple (suite)

- Comme `freqTexte(mystere,10,0)` nous indique 18% de ‘p’ et 11% de ‘w’, on peut faire l’hypothèse que l’espace est codé par ‘p’ et le ‘e’ est codé par ‘w’.
- Ceci est cohérent avec un codage par la lettre ‘s’. La longueur de la clef est donc 10 et sa première lettre est ‘s’.
- On regarde maintenant `freqTexte(mystere,10,1)` et on trouve de la même façon la seconde lettre de la clef : ‘c’.

# Un exemple (fin)

- Après avoir fait de même pour les autres lettres, on a trouvé la clef : schweitzer.
- On peut alors décoder et après avoir rétabli les majuscules on obtient :

# La réponse

- Après avoir obtenu une licence en Mathématiques, **Margaret Hamilton** (née en 1936) intègre le **MIT** (Massachusetts Institute of Technology) et commence à y développer des programmes de prévision météorologique ainsi que des programmes de détection d'avions pour l'armée américaine. En 1960, à l'âge de 24 ans, elle est repérée et recrutée par la NASA pour le poste de **Directrice du Département Génie Logiciel**… soit le département en charge de programmer les logiciels servant à la navigation et à l'alunissage qui seront embarqués dans les vaisseaux spatiaux de lamission **Apollo 11,** 9 ans plus tard !
- Grâce à ses idées novatrices notamment en matière de **systèmes d'interface homme-machine** et en techniques d'**automatisation de cycle de vie des applications**, la mission fut couronnée de succès et l'alunissage a pu avoir lieu sans encombre. En effet, quelques minutes seulement avant que le module lunaire ne touche la surface du sol, un défaut de fonctionnement du système lié à la gestion de trop nombreuses tâches en simultané est détecté par l'ordinateur de bord qui parvient à le corriger automatiquement en ne priorisant que les tâches les plus importantes.
- À la manière d'un auto-diagnostic de l'ordinateur puis un Crtl+Alt+Suppr et "fin de tâche" automatique, ce qui était une **avancée phénoménale** en terme de programmation pour l'époque ! Il aura fallu attendre 47 ans après que Neil Armstrong ait posé le pied sur la Lune pour que **Margaret Hamilton** soit décorée en 2016 de la Médaille Présidentielle de la Liberté par Barack Obama.
- (source : https://www.jems-group.com/recrutement/actualites/4-femmes-scientifiques-qui-ont-revolutionne-linformatique/ )