Jean-Michel Masereel
Valérie Nachef
Emmanuel Volte

Évolution de la cryptographie à travers les âges

Cours, exercices corrigés, algorithmes en Scratch et Python

ellipses

1. La cryptographie dans l'Antiquité

Les écritures secrètes semblent être nées spontanément dès que, dans un pays, une partie importante de la population a su lire. En effet, tant que la lecture a été réservée à une petite partie de la population, il n'y avait pas un réel besoin de cryptographie. Ceci a été le cas en Égypte et en Chine. En 1900 av. J.-C., dans une ville nommée Menet Khufu, au bord du Nil, un scribe égyptien a employé des hiéroglyphes non conformes à la langue correcte dans une inscription sur une stèle funéraire relatant la vie de son maître. C'est parfois présenté comme un premier exemple de cryptographie. Cependant le but de ce procédé n'était pas de rendre le texte incompréhensible mais plutôt de le rendre plus solennel. En Chine, c'est la stéganographie qui a été davantage utilisée : le message n'est pas rendu incompréhensible par un procédé de chiffrement mais écrit sur du papier ou de la soie, roulée en boule et recouvert de cire. Le porteur dissimulait la sphère de cire sur lui ou avalait celle-ci. La stéganographie a été également utilisée aux alentours de 600 av. J.-C. par Nabuchodonosor, roi de Babylone : il écrivait le message sur le crâne rasé de ses esclaves, attendait que leurs cheveux aient repoussé, et il les envoyait à ses généraux. Il suffisait ensuite de raser à nouveau le messager pour lire le texte.

1.1. Le plus ancien document chiffré de l'Antiquité

Le premier « document » chiffré connu remonte à l'Antiquité. Il s'agit d'une tablette d'argile, retrouvée en Irak, et datant du XVI^{e} siècle av. J.-C. Un potier y avait gravé sa recette secrète pour appliquer du vernis sur les poteries en supprimant des consonnes et en modifiant l'orthographe des mots.

FIGURE 1.1. – Premier document chiffré

1.2. Petite histoire de l'alphabet

1.2.1. L'évolution de l'alphabet

Les premiers alphabets phonétiques qui ont été utilisés du XX^e^ au VIII^e^ siècle av. J.-C. étaient des systèmes syllabiques. Par exemple, l'écriture des Assyriens utilisait un syllabaire de 500 signes cuneïformes. Puis apparaissent les alphabets consonantiques, avec vers 1100 av. J.-C., un alphabet de 22 consonnes, probablement élaboré à Byblos. Le timbre des voyelles était imposé par le rôle du mot dans la phrase. L'alphabet des Phéniciens se diffuse ensuite dans tout le bassin méditerranéen à partir du VIII^e^ siècle av. J.-C. : d'abord à Chypre et à Carthage, puis en Afrique du Nord et en Espagne. Inspiré de l'alphabet phénicien, l'alphabet grec est le premier à introduire les voyelles. On estime qu'il a dû être conçu vers 900 av. J.-C. Les Grecs ont repris les signes phéniciens pour noter les consonnes et ont ajouté des signes pour noter les voyelles. Cet alphabet a ensuite servi de modèle aux futurs alphabets latin et cyrillique.

Ce sont les Étrusques, en contact avec les Grecs, qui conçoivent un alphabet vers 700 av. J.-C., qui sera utilisé en Italie et répandu par les Romains dans le monde méditerranéen. Dans cet alphabet latin, les débuts de lettres grecques sont conservés : alpha devient a, béta devient b (prononcé bé). Certains signes ont été abandonnés (consonnes aspirées) ou transformés. La lettre G a été créée pour la différencier de la lettre C selon la prononciation. Le Y et le Z ont été repris pour les mots d'origine grecques. On en était alors à 23 lettres.

Au XVI^e^ siècle, on a 23 lettres dans l'alphabet. Les lettres J, V et W n'existent pas ainsi que les accents, le tréma et la cédille. De plus, il y a peu de signes de ponctuation. En 1542, le grammairien Louis Meigret propose d'introduire la lettre J pour faire une distinction entre les sons « i » et « j » qui jusque là étaient représentés tous les deux par la lettre i. Puis, en 1548, Ervé Fayad,

propose de distinguer les sons « u » et « v » qui étaient représentés par la lettre u uniquement. La lettre v apparaît.
En 1762, dans la quatrième édition de son dictionnaire, l'Académie sépare i et j, ainsi que u et v.
L'introduction du W a été plus compliquée. Il a été crée par doublement du V pour représenter le [w] germanique. Dans les premières éditions du dictionnaire de l'Académie, aucun mot orthographié avec la lettre W n'est présent. Les premiers mots ayant un W sont isolés dans le dictionnaire de 1878 car on considère que W est une lettre étrangère. En 1964, il est écrit dans le Robert que W est la 23^{e} lettre de l'alphabet, ce qui donne 26 lettres dans l'alphabet.

1.2.2. L'alphabet et la mythologie

Europe était une princesse phénicienne, fille d'Agénor roi de Tyr. D'après la légende, alors qu'elle se promenait au bord de la mer, elle fut enlevé par Zeus qui s'était transformé en taureau. Ils parvinrent en Crète où Zeus s'unit à Europe. Trois fils naquirent ce cette union : Minos, Sarpedon et Rhadamante. Un des frères d'Europe, Cadmos, partit à sa recherche avec interdiction par son père de revenir tant qu'il n'aurait pas trouvé Europe. Il alla en Grèce interroger l'orale de Delphes. L'oracle lui conseilla de suivre une génisse errante et de fonder une ville à l'endroit où elle se coucherait épuisée. C'est ainsi qu'il se rendit au site de Thèbes où il fonda Cadmée. Selon la légende, pour retrouver sa sœur, il offrit également aux Grecs l'alphabet inventé par les Phéniciens. N'ayant pas retrouvé Europe, il ne rentra jamais à Tyr.

1.3. Le procédé « Atbash », 500 av. J.-C.

Au V^{e} siècle av. J.-C., des scribes hébreux mettant par écrit le livre de Jérémie ont employé un chiffrement de substitution simple connu sous le nom d'Atbash. Ce procédé consiste à faire correspondre l'alphabet classique avec l'alphabet inversé, et d'associer ainsi à chaque lettre la lettre correspondante en position dans l'alphabet inversé. Par exemple, avec l'alphabet latin, le A est chiffré en Z, le B en Y et ainsi de suite. Le nom du système dérive de son fonctionnement, puisqu'il est constitué à partir des lettres aleph, tau, beth et shin, qui sont les deux premières (aleph et beth) et les deux dernières (shin et tau) lettres de l'alphabet hébreux. Le chiffrement Atbash est représenté dans la table 1.1.

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

TABLE 1.1. – Chiffrement « Atbash »

Il existe deux procédés de substitution très similaires qualifiés de chiffre « Albam » et chiffre « Atbah ». Dans le procédé Albam (table 1.2), il y a un décalage des lettres de 13 positions.

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

TABLE 1.2. – Chiffrement « Albam »

Dans le procédé Atbah (table 1.3), on regroupe les lettres par groupes de 4. Les lettres A,B,C, D sont associées aux lettres F, G, H, I et ordonnées à l'envers. Il en est de même pour les lettres J, K, L, M et les lettres O, P, Q, R puis les lettres S, T, U, V et les lettres W,X,Y,T. Les lettres E et N sont échangées.

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

TABLE 1.3. – Chiffrement « Atbah »

1.4. La scytale spartiate, 400 av. J.-C.

Le premier dispositif de cryptographie militaire connu, la scytale spartiate, remonte au V^e^ siècle av. J.-C.. La scytale consiste en un bâton de bois autour duquel est entourée une bande de cuir ou de parchemin, comme le montre la figure 1.2. L'expéditeur écrit son message sur toute la longueur de la scytale et déroule ensuite la bande qui apparaît alors couverte d'une suite de lettres sans signification. Le messager emportera la bande de cuir, l'utilisant comme ceinture, les lettres tournées vers l'intérieur. Le destinataire enroulera alors cette bande sur son bâton (de même diamètre) pour lire le message clair. Ce procédé de chiffrement est un chiffrement par transposition. On bouleverse l'ordre des lettres de façon à rendre le texte incompréhensible mais on ne remplace pas les lettres du message par d'autres lettres ou symboles. Le texte clair et le texte chiffré auront donc la même fréquence de lettres.

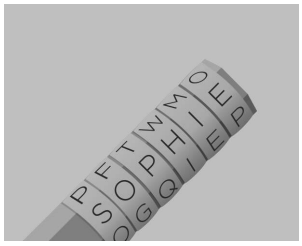

FIGURE 1.2. – Scytale spartiate

Ce dispositif a été utilisé par Lysandre de Sparte [26]. Lors de la bataille d'Aigos Potamos en 405 av. J.-C., la flotte spartiate commandée par Lysandre de Sparte avait complètement détruit la flotte athénienne. Pharnabaze, satrape perse, en charge des côtes d'Asie Mineure avait soutenu Lysandre de Sparte durant cette guerre contre Athènes. Cependant, Lysandre, installé dans le nord de Sparte à Sestos, se demandait s'il devait toujours considérer les Perses comme des alliés. Des troubles avaient éclaté dans des villes et il pensait que la Perse n'y était peut-être pas étrangère. Il devait savoir quel parti prendre et quelle décision le gouvernement de Sparte attendait de lui. Fallait-il déclencher une guerre contre Sparte sans y être préparé ou laisser les villes prendre une expansion qui ne pourrait plus être maîtrisée ? En 404 av. J.-C., Lysandre vit arriver un messager ensanglanté. Il était le seul rescapé d'un groupe de quatre porteurs de messages envoyés de Sparte. Le messager tendit sa ceinture à Lysandre qui l'enroula autour de sa scytale. Il apprit ainsi que Pharnaze de Perse s'apprêtait à l'attaquer. Il put alors se préparer et repousser l'attaque.

C'est le premier emploi de la cryptographie mentionné dans l'histoire et qui a permis de sauver un général et son empire.

1.5. Le carré de Polybe, 200 à 125 av. J.-C.

Polybe est un historien grec qui a vécu aux environs de 200-125 av. J.-C. Il est à l'origine du premier chiffrement par substitution. On utilise un carré de 25 cases (5×5). On peut agrandir ce carré si on veut ajouter des chiffres ou si l'alphabet utilisé comprend davantage de lettres. Le carré de Polybe est représenté dans la table 1.4. En français, on supprime la lettre « W ». En anglais, on regroupe le I et le J. Chaque lettre est représentée par un groupe de deux chiffres : celui de sa ligne et celui de sa colonne. Ainsi E = 15, U = 51, N = 34,... Polybe proposait de transmettre ces nombres au moyen de torches. Une torche à droite et cinq à gauche pour transmettre la lettre « E » par exemple. Ce procédé permettait donc de transmettre des messages sur de longues distances. On peut aussi transmettre les coordonnées des lettres en tapant des coups sur un mur, sur la tuyauterie, etc.

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

TABLE 1.4. – Carré de Polybe

Ce mode de chiffrement peut être amélioré en utilisant un mot-clef partagé par l'expéditeur et le destinataire. On commence à remplir le carré à l'aide des lettres du mot-clef et on continue le remplissage à l'aide des lettres de l'alphabet écrites dans l'ordre alphabétique mais en supprimant les lettres du mot-clef. Ainsi, avec le mot-clef POLYBE, le carré obtenu est donné dans la table 1.5. L'analyse des fréquences permet de casser ce code qui ne fut pas utilisé car il était trop compliqué. Cependant comme nous le verrons plus tard, des améliorations de ce code seront utilisées par l'armée allemande durant la Première Guerre mondiale.

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

TABLE 1.5. – Carré de Polybe avec mot-clef

1.6. Le code de Jules César, 60 av. J.-C.

Durant l'Antiquité, le premier procédé de chiffrement utilisé par les Romains, fut inventé par Jules César pour une utilisation militaire. Pour coder les messages, il suffisait de décaler les lettres de l'alphabet de trois rangs. Ainsi, la lettre A est codée par la lettre D, la lettre B par la lettre E et ainsi de suite. Ce mode de chiffrement fut encore utilisé par les officiers sudistes durant la guerre de Sécession et aussi par l'armée russe en 1915.

On remarque cependant, que si l'on sait que l'on a utilisé un chiffrement par décalage, il suffit d'essayer tous les décalages possibles jusqu'à ce que l'on obtienne un texte qui a du sens. Donc la recherche exhaustive de clefs est, dans ce cas, très facile. Cependant, à cette époque, le nombre de personnes sachant lire était très restreint et donc cela pouvait apporter une certaine sécurité au code.

Les chiffrements Atbash, Albam, Atbah, ainsi que celui de Jules César, font tous partie de la famille des chiffrements par substitution.

1.7. Exercices

Activité 1.1 (College)**.** Pour faciliter le chiffrement par décalage, on peut proposer une activité consistant à écrire toutes les lettres de l'alphabet, de façon régulière autour de deux cercles de rayon 5 cm et 7 cm par exemple. L'exercice n'est pas si facile car 360 n'est pas divisible par 26, et des erreurs qui se cumulent peuvent donner un décalage non négligeable à la fin. Pour simplifier, on peut omettre les lettres J et W (en les remplaçant respectivement par I et V), ce qui donne 24 lettres, et il faut donc placer une lettre tous les 15 degrés.

Une fois les cercles construits, et éventuellement coloriés de couleurs différentes, on les découpe, on met le plus petit sur le plus grand et on les attache au milieu à l'aide d'une attache parisienne.
On peut remarquer que le même outil peut servir pour le chiffrement et le déchiffrement, sans changer la position des cercles, mais en l'utilisant d'une façon différente. C'est déjà une façon de représenter une fonction et de chercher image et antécédent, sans forcément employer le vocabulaire.
Remarque : Une illustration, réalisée avec Scratch est donnée au chapitre suivant (disque d'Alberti)

Activité 1.2 (primaire, collège)**.** On peut se lancer dans la fabrication d'une scytale. Le plus simple est d'utiliser des rouleaux vides de papier absorbant, ou des rouleaux pour du papier cuisson. Il est important que ces rouleaux soit assez longs et suffisamment solides. Un tuyau en PVC pourrait également convenir.

Le plus délicat est de fabriquer une bande. On peut par exemple découper des bandes de 2 cm de largeur et les scotcher les unes après les autres afin d'obtenir une bande assez grande. Une autre idée serait de récupérer une lanière de cuir assez régulière mais il est alors compliqué de l'utiliser plusieurs fois.

Dans tous les cas, on s'aperçoit qu'il n'est pas si facile d'enrouler de manière régulière la bande autour du rouleau. Il faut écrire le message en espaçant bien les lignes.

Voici différentes situations pédagogiques pour utiliser la scytale :

— Demander à un petit groupe de faire un exposé autour de la scytale et de fabriquer une scytale, par exemple pour un projet de fin d'année.
— Dans un escape game. Il faudra que le rouleau à utiliser soit bien visible, ou bien s'arranger avec un jeu de couleur pour que l'association entre la bande et le rouleau soit évidente.

Exercice 1.3. Le texte suivant est un extrait d'un roman qui a été chiffré par un chiffrement mono-alphabétique. Quel est le titre du roman (dernière phrase) ?

XZCLQJLC AVN YTCHZFL BZC BZVYNYT. WT C'TQLNQ EVT UZANQTBBT. YNTC RT QZVQ WL CT O'NOUZYQT, UTCBLNQ-NA, XVBEV'L WT EV'NA BT YTCRT WZOUQT, LHTW VCT TWZTVYLCQT WTYQNQVRT, L EVTA UZNCQ W'TQLNQ GLVK. NA CT HZVALNQ ULB BT YT-