**LES FICHES DU CLUB ALKINDI**

## PRÉSENTATION ET PLAN DES FICHES

### 1. PRÉSENTATION DES FICHES :

Ces fiches ont été rédigées spécialement pour vous *initier à la cryptographie* et vous donner l'envie de vous amuser à déchiffrer des messages secrets. Au début, ce sera un jeu, puis si vous y prenez goût, cela deviendra une passion. Éventuellement cela pourra devenir votre métier.

Cette initiation aura un aspect principalement historique : nous étudierons les deux principales méthodes de chiffrement, *la substitution* (remplacement des lettres par d'autres lettres, des chiffres ou des symboles) et *la transposition* (mélange des lettres selon une méthode prédéfinie). Nous verrons également *les systèmes de codage et les dictionnaires.*

Cet aspect historique est fondamental. Pour bien débuter dans le monde de la cryptographie, il est indispensable d'apprendre comment, au cours des siècles, ont évolué les méthodes pour cacher aux ennemis ou aux simples tiers les messages que l'ont adresse à ses amis ou ses alliés. Cela permet de s'initier au jargon bizarre de la cryptographie : chiffrement, clé, analyse fréquentielle, casser un code, système RSA... (ces mots seront définis au fur et à mesure). Mais surtout, cette histoire permet de comprendre l'extraordinaire révolution de la cryptographe moderne, la rupture brutale qui s'est effectuée au cours des années 1980, rupture qui a balayé tous les anciens concepts, et les nouveautés qui en ont résulté : protection des données dans les ordinateurs, communications dans les réseaux sociaux, utilisation privée dans les cartes bancaires etc.

Le système de *« fiches » écrites* a été volontairement choisi. En effet, il existe de nombreuses vidéos sur YouTube, bien réalisées, attrayantes, qui donnent des cours de cryptographie. Mais au départ, pour vraiment comprendre et progresser dans ce domaine, il faut avoir devant soi un papier et un crayon, écrire, chercher et finalement trouver la solution. C'est comme l'histoire-géo, les maths ou le sport , ça ne vient pas tout seul : il faut bosser, faire des exercices, s'entraîner. Des sites Internet vous proposent de déchiffrer automatiquement des messages secrets. Ces sites sont remarquablement faits, mais encore faut-il savoir comment les utiliser, et déterminer à quel type de message on a affaire. Et là, seule la pratique concrète des recherches avec un papier, un crayon, une simple calculatrice vous permettra d'utiliser efficacement ces sites. On peut aussi se servir d'Excel ou créer des programmes Python, mais là encore il faut connaître et comprendre les modes de chiffrement de base. Les énigmes du Club Alkindi sont là pour vous amuser, mais aussi pour vous y entraîner. Et vous découvrirez le plaisir de trouver la solution, de déchiffrer un message secret.

Ces fiches sont évolutives : elles sont éditées en fichiers pdf, et on peut facilement les modifier, supprimer une ancienne fiche, y substituer une nouvelle. Bien entendu vous pouvez les télécharger. N'hésitez pas à poser des questions et à signaler des erreurs ou des améliorations possibles, les échanges nous permettront de progresser.

Il existe sur le sujet quelques livres très bien faits, et d'autres un peu moins bons. Nous les évoquerons, et nous pourrons échanger des avis. Il existe également de nombreux sites Internet, et quelques films. Là aussi nous en parlerons tous ensemble.
A suivre…

## 2. PLAN DES FICHES :

Ce plan est donné à titre indicatif. Il donne une structure générale, avec quelques données incontournables, et suit une évolution historique. Il essaye également d'être le plus pédagogique possible. Mais il n'est pas figé et sera modifiable : l'auteur peut faire des erreurs, il apportera des modifications et des améliorations, et les lecteurs pourront demander à approfondir tel ou tel point.

### Fiche 1. A quoi sert la cryptographie ?

Jusqu'au milieu du XXe siècle, le secret des messages concerne principalement les militaires et les diplomates.
Le problème de fond : communiquer en sécurité, c'est à dire donner une information à un ami en cachant cette information à tous les autres.
Lutte constante entre les chiffreurs et les déchiffreurs : créer une méthode secrète, la découvrir.

Les deux méthodes de base du chiffrement : substitution et transposition.

- *Substitution* = remplacement d'une lettre par une autre lettre, un nombre ou un symbole - *Transposition* = mélange des lettres selon une méthode prédéfinie.
Exemples : substitution simple lettre à lettre, transposition par une grille.

- Il existe aussi *les codes et les dictionnaires.*

### Fiche 2. Les chiffrements par substitution

Définition des termes **:** clair, algorithme, cryptogramme, ...

- Le chiffrement par substitution simple

Historique :
- Le chiffre de Jules César (1$^{er}$ siècle av J-C)
- Inversion de l'alphabet : l'Atbash dans la Bible hébraïque
- Méthodes basiques de substitution : une lettre, un nombre ou un symbole remplacent une lettre.

- Le chiffrement par bigrammes **:** Le carré de Polybe (150 av J6C)

- Les méthodes classiques de substitution simple

- Comment décrypter ? : l'analyse de fréquence, AlKindi (IXe siècle)

- Neutraliser l'analyse de fréquence : Le chiffre de Vigenère (XVIe siècle) :

  - Fondamental, introduit le concept de clef : clair + clef = crypto
  - L'utilisation de la clef permet de casser la fréquence des lettres
  - Mais on peut parvenir à décrypter en cherchant la longueur de la clé (Babbage)

- Le chiffre inviolable **:** le concept de clé aléatoire utilisée une seule fois.

- Inconvénient des clefs aléatoires « une fois » : lourdeur de la méthode, difficulté et risque dans la communication de la clef aux amis.

- Le principe de Kerckhoffs  (1883) : la sécurité d'un système de chiffrement ne doit reposer que sur le secret de la clef et non pas sur l'algorithme de chiffrement, qui peut être connu de l'ennemi.

**Fiche 3.  On reste dans l'Histoire : les codes, les dictionnaires** : une forme de substitution

Les codes : le Morse, le système binaire, l'ASCII, l'alphabet radio international : ce sont des façons de coder, *ce n'est pas de la cryptographie*, il n'y a rien de caché.

Les codes et les dictionnaires : Exemples : le chiffre des Templiers, Marie Stuart, le Grand Chiffre de Louis XIV etc.

**Fiche 4. Les chiffrements par transposition :**

- Très en vogue dans le monde militaire et employé au XIXe siècle jusqu'à la Seconde Guerre mondiale. Très efficace. Mais aussi quelques inconvénients.

Exemples :
- la scytale spartiate ou bâton de Plutarque (- 600 av. J-C)
- le chiffre *rail fence* ou zig zag
- les grilles
- le chiffre Übchi
- le chiffre ADFGX : *substitution,* puis *surchiffrement* au moyen d'une *transposition*
- Littérature :  Jules Verne, Voyage au centre de la terre.

**Fiche 5. L'évolution pendant la Seconde Guerre mondiale : Enigma**

Comme d'habitude, hélas, les guerres font des morts, mais font faire aussi d'immenses progrès dans tous les domaines. On reste dans la substitution, mais complexification : on entre dans l'ère des machines électromécaniques, ancêtres des ordinateurs (la « bombe » d'Alan Turing pour déchiffrer Enigma), Dans le concours Alkindi, il y a des énigmes avec des machines (figurées!)

**Fiche 6. Une rupture radicale : le système RSA (1975)**

Petits rappels de maths : les nombres premiers, les fonctions à sens unique (arithmétique  Modulo), la fonction puissance (définition),

Les précurseurs : Le système Diffie,Hellmann, Merke

Le système RSA : Ronald Rivest, Adi Shamir et Leonard Adleman

Révolution complète dans ces méthodes de chiffrement : aucune clef n'est échangée avec le destinataire. Concepts de clef symétrique et asymétrique, clef publique et clef privée.

**Fiche 7. Que faire face à une énigme ?**
- Des chiffres ? Des lettres ? On est face à quel type de chiffrement ?
- Exemples
- Trouver l'algorithme, la clef ?
- L'environnement, les indices, les mots probables
- L'importance de travailler en équipe si l'on peut

**Fiche 8. Les livres, les sites Internet, les films**