Université de Nîmes. TP proposé par M. Brouzet

# TP 1 : Deux systèmes cryptographiques historiques

**Manip 1 Le chiffre de Jules César**

L'historien Suétone rapporte dans son ouvrage « Vie des douze César » que Jules César utilisait, pour communiquer, des messages cryptés. Sa méthode consistait à décaler les lettres de l'alphabet de trois lettres [1] vers la droite [2], le « A » se transformant ainsi en « D », le « B » en « E » etc. Ce procédé est connu désormais sous le nom de *chiffre* [3] *de Jules César*. Il peut bien sûr se pratiquer avec d'autres décalages ; on a alors un même procédé cryptographique (une même recette : ici décaler l'alphabet) mais qui s'applique avec diverses valeurs d'un paramètre (ici le nombre de lettres dont on décale l'alphabet) ; ce paramètre, soit $k$, est appelé la *clé* du système cryptographique. Bien sûr, cette clé doit être communiquée au destinataire afin qu'il puisse faire le décryptage du message, mais doit être tenue *secrète* pour toute personne non autorisée à lire le message.

A vous de jouer :

1. Dans la description ci-dessus il y a un non-dit, un implicite qu'il convient d'éclaicir. En effet, si on décale par exemple de trois crans vers la droite l'alphabet écrit en ligne de gauche à droite, que deviennent donc les trois dernières lettres X,Y et Z ? Dans ce cas, quelle figure géométrique serait plus adaptée que la « ligne » pour disposer l'alphabet ?

2. Cryptez suivant le procédé de Jules César, avec $k = 11$, le message suivant :

LES VACANCES SONT TERMINEES

3. Décryptez le message suivant que vous a transmis Jules César avec $k = 3$ :

YHQL YLGL YLFL

4. Vous avez intercepté le message suivant crypté par le procédé de Jules César mais dont vous ignorez la clé. Essayez de le décrypter tout de même (on dit dans ce cas que vous faites de la cryptanalyse) :

MOVK OCD ZVEC PKMSVO AEO ZBOFE

**Manip 2 Le chiffre de Vigenère**

Blaise de Vigenère, écrivain et diplomate du seizième siècle, imagina le procédé cryptographique suivant, qualifié depuis de, *chiffre de Vigenère*. La *clé secrète* est cette fois un mot, par

1. Le blanc ou espace n'est pas considéré ici comme une lettre et on utilise donc l'alphabet standard à 26 lettres.
2. Cela sous-entend que l'on a écrit les lettres de A à Z en ligne de gauche à droite.
3. Le mot « chiffre » ("cypher" en anglais) est synonyme ici de cryptage ou procédé cryptographique et ne renvoie pas aux chiffres qui servent à écrire les nombres.

exemple le mot « DUR », et le procédé consiste à appliquer un décalage de Jules César variable suivant la position de la lettre dans le message ; précisément on décale la première lettre du message suivant « A » donne « D », la deuxième suivant « A »donne « U », la troisième suivant « A » donne « R », la quatrième suivant « A »donne « D » à nouveau etc. Là encore, on ne considère pas le blanc ou espace comme une lettre et on travaille avec un alphabet standard de 26 lettres.

A vous de jouer :
Décryptez le message que vous a envoyé Blaise (le mot clé est « SECRET ») :

UI VVBMW IUK MEDMUZFEW

**Manip 3 Cryptage et arithmétique modulaire**
Au lieu de travailler avec des lettres, numérotons les (en partant de 0) comme nous l'avons vu lors du TP 1. Ainsi, si nous travaillons avec un alphabet de 26 lettres et ignorons l'espace, le « A » correspondra à 0,..., le « Z » correspondra à 25, et si nous travaillons avec l'alphabet standard augmenté de l'espace, nous pourrons numéroter de manière naturelle le blanc par 0, le « A » par 1,..., le « Z » par 26.

1. Pourriez-vous définir, de manière commode, une règle d'addition sur ces "numéros" de lettres, qui corresponde au décalage circulaire des lettres pratiqué dans le procédé de Jules César ?

2. Notons $\mathbb{Z}_{26}$ (ou $\mathbb{Z}_{27}$ selon l'alphabet utilisé) ces ensembles de "numéros de lettres", munis de la règle d'addition précédente.

   a) Donnez une application de cet ensemble dans lui-même décrivant un décalage de Jules César de 3 crans ; de 11 crans.

   b) Quelles applications correspondent alors aux opérations de décryptage ?

3. En exploitant ce formalisme, sauriez-vous alors donner une application décrivant un cryptage de Vigenère de votre choix, ainsi que celle correspondant au décryptage ?