**MPS : Mathématiques – Cryptographie.**
**SEANCE 1**

## 1. Qu'est-ce que la cryptographie

Lire le texte donné en ANNEXE 1 : « Origines de la cryptographie »

## 2. Premier exemple de codage : le code césar

### a. Principe

D'après le texte précédent, en quoi consiste « le code César » ?

### b. Automatisation du cryptage

En informatique, le code ASCII consiste à associer à chaque caractère (lettre de l'alphabet, signe de ponctuation, espace, ….) un code numérique que l'on appelle son code ASCII
Pour les lettres majuscules : A est codé par 65, B par 66, C par 67 , etc……

| **lettres** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | Y | X | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Code ASCII** | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |

A chaque lettre de l'alphabet, on associera son rang dans l'alphabet (ainsi 1 est associé à A, 2 est associé à B, etc…).

| **lettres** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | Y | X | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **rang** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Nous allons construire un automate qui permet de crypter un message avec une clé quelconque.

**Préparation des formules à saisir sur tableur :**

Sur tableur, la formule « =**code(A)** » affiche 65 , c'est-à-dire le code ASCII de A
la formule « =**car(66)** » affiche B, c'est-à-dire le caractère associé au code ASCII 66.

1) Si on note x le code ASCII, d'une lettre, quelle formule permet d'obtenir son rang dans l'alphabet ?

2) On suppose dans cette question que la clé est égale à +12
   a) En quels nombres sont transformés les rangs des caractères « A », « R » et « V » lors du cryptage de César ?

   On note MOD(n ;26) le reste de la division euclidienne d'un entier n par 26.

   b) Calculer MOD(12 ;26), MOD(29 ;26) et MOD(33 ;26)

   c) Si on appelle $x$ le rang du caractère à chiffrer, vérifier à l'aide des caractères « A », « R » et « V » que la formule " $= MOD(x + 12; 26)$" donne le rang du caractère crypté.

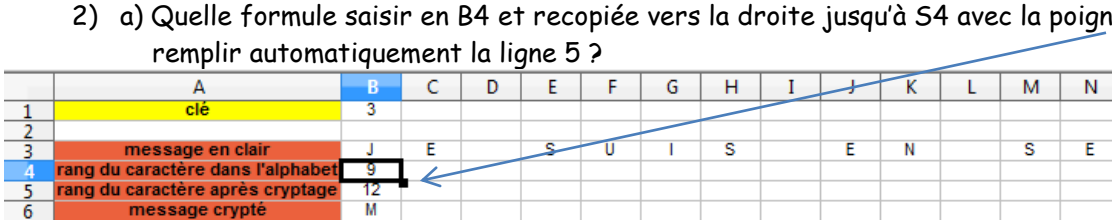
Sur tableur, la formule « =MOD( *nombre* ; 26) » donne le reste de la division euclidienne de *nombre* par26.

3) Si on note y le rang dans l'alphabet d'une lettre, quelle formule permet d'obtenir son code ASCII ?

**Création de l'automate sur tableur :**

1) Dans le site http://www.lewebpedagogique.com/sfeulvarch/ , rubrique : MPS, ouvrir la feuille de calcul

2) a) Quelle formule saisir en B4 et recopiée vers la droite jusqu'à S4 avec la poignée de recopie pour remplir automatiquement la ligne 5 ?



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | clé | 3 | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | | |
| 3 | message en clair | J | E | | S | U | I | S | | E | N | | S | E | C | O | N | D | E |
| 4 | rang du caractère dans l'alphabet | 9 | | | | | | | | | | | | | | | | | |
| 5 | rang du caractère après cryptage | 12 | | | | | | | | | | | | | | | | | |
| 6 | message crypté | M | | | | | | | | | | | | | | | | | |

b) Mêmes questions pour B5 (attention la clé est saisie en B1) et B6.

Vous obtiendrez le résultat suivant :

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | clé | 3 | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | | |
| 3 | message en clair | J | E | | S | U | I | S | | E | N | | S | E | C | O | N | D | E |
| 4 | rang du caractère dans l'alphabet | 9 | 4 | | 18 | 20 | 8 | 18 | | 4 | 13 | | 18 | 4 | 2 | 14 | 13 | 3 | 4 |
| 5 | rang du caractère après cryptage | 12 | 7 | | 21 | 23 | 11 | 21 | | 7 | 16 | | 21 | 7 | 5 | 17 | 16 | 6 | 7 |
| 6 | message crypté | M | H | | V | X | L | V | | H | Q | | V | H | F | R | Q | G | H |

c. Automatisation du décryptage

1) On suppose que la clé est 12.

Si on appelle $y$ le rang du caractère crypté, vérifier à l'aide des caractères « M », « D » et « H » que la formule " $= MOD(y - 12; 26)$" donne le rang du caractère avant cryptage.

2) Saisir les formules nécessaires à recopier vers la droite pour décrypter un message dans la feuille de calcul nommée « décryptage ».

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | clé | 3 | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | | |
| 3 | message crypté | M | H | | V | X | L | V | | H | Q | | V | H | F | R | Q | G | H |
| 4 | rang du caractère crypté dans l'alphabet | 12 | | | | | | | | | | | | | | | | | |
| 5 | rang du caractère dans l'alphabet avant cryptage | 9 | | | | | | | | | | | | | | | | | |
| 6 | message en clair | J | | | | | | | | | | | | | | | | | |

d. Codage et décodage grâce au code César

Ecrire un message en majuscule sans ponctuation sur une feuille de papier et le coder grâce à la feuille de calcul nommée cryptage et le noter sur une deuxième feuille de papier.
Ensuite, échanger les messages codés entre les groupes. Et tenter de décrypter le message reçu avec la feuille de calcul décryptage. Vérifier avec le groupe qui vous a remis le message.

e. Essai de décryptage du message retrouvé sur le lieu du crime.

En ANNEXE 2, vous trouverez un indice trouvé sur le bureau de la victime : un message codé.
En utilisant la feuille de calcul « message bureau », pouvez-vous le décrypter avec cette méthode ?

f. Limites d'un tel codage

Pour un texte donné, combien de codages différents peut-on faire ?
Quelles idées pour améliorer ce codage ?

g. Fiche de synthèse

On demande de réaliser une fiche synthèse sur le code césar donnant le principe de ce cryptage, un exemple et les limites de ce codage.
A la fin de cette fiche, vous devrez faire apparaitre votre conclusion sur l'indice étudié.

**Un très bon site pour les plus rapides : http://www.apprendre-en-ligne.net/crypto/menu/index.html**

ANNEXE 1 : ORIGINES DE LA CRYPTOGRAPHIE

# Dans l'Antiquité, les rives de la Méditerranée ont connu de nombreuses guerres. La cryptographie est née de la nécessité de conserver le secret des communications entre les chefs militaires et leurs armées, ainsi qu'entre les États qui avaient noué des alliances.

Contrairement à la stéganographie qui s'efforce de dissimuler l'existence d'un message, la cryptographie (du grec *graphein* et *cryptos* : « écriture cachée ») cherche à en dissimuler le contenu.

## La scytale de Sparte

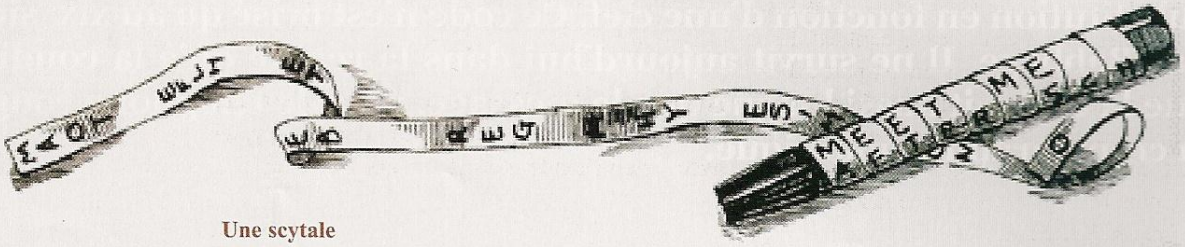
Si on en croît ce qui est écrit par l'historien grec Plutarque (47-120 après J.-C.), la cryptographie serait née à Sparte au V^e^ siècle avant notre ère. Pour transmettre des messages confidentiels entre les magistrats de la cité et les généraux en campagne, les Spartiates utilisaient deux bâtons de même longueur et de même diamètre, les scytales. L'un des bâtons restait à Sparte tandis que l'autre était emporté par le général. Pour crypter un message, on enroulait en spires jointives un mince bandeau de papyrus (ou de parchemin) sur l'un des bâtons puis on y écrivait le message à protéger. Une fois déroulée, la bande qui ne présentait plus qu'un texte d'apparence incohérente pouvait être acheminée vers son destinataire. Pour lire le message, celui-ci devait enrouler la bande autour du second bâton afin de reformer le texte en clair.

Pour illustrer ses dires, Plutarque rapporte qu'en 404 avant Jésus-Christ, le général spartiate Lysandre vit arriver, venant de Perse, un messager qui lui tendit sa ceinture. Lysandre l'enroula autour de sa scytale et, déchiffrant le message qui lui était envoyé, apprit que les Perses s'apprêtaient à l'attaquer.

## Les méthodes d'Enée le tacticien

Énée le Tacticien était un des généraux de la Ligue Arcadienne qui, au IV^e^ siècle avant Jésus-Christ, regroupait un certain nombre de cités grecques. Il a écrit plusieurs ouvrages sur l'art militaire dont un seul nous est parvenu. Il s'agit d'un traité intitulé *Poliorcétiques* qui concerne principalement la défense de la cité mais aussi l'art de crypter des messages. Énée nous apprend par exemple à remplacer les voyelles du texte à cacher par des points : un pour *alpha*, deux pour *epsilon* et ainsi de suite jusqu'à sept pour *omega*. Les consonnes, quant à elles, restent inchangées. Avec ce procédé, le message DENIS EST HONNÊTE devient D..N...S ..ST H....NN.T..

Il explique comment camoufler un texte en insérant des lettres quelconques entre celles du texte à protéger. Des marques presque invisibles, des



Une scytale

trous minuscules en général, doivent être faites pour signaler au destinataire du message les lettres à utiliser.

Au lieu de trous, utilisons par exemple une couleur pour transformer le message DENIS EST HONNÊTE en DARESTFNZAQIS EKLSZT HPTONKKKNÊDTE. Dans le message transformé, seules les lettres en rouge sont à prendre en considération.

Une troisième méthode consiste à percer 24 trous, un trou par lettre, dans un osselet ou dans un morceau de bois. Le chiffrement consiste alors à passer un fil à travers les trous qui représentent les lettres du message à envoyer. Pour déchiffrer le message, il faut naturellement connaître l'ordre des trous en partant de celui qui indique l'alpha.

## Le chiffre de Jules César

En 58 avant Jésus-Christ, Jules César se lançait à la conquête de la Gaule. Pour communiquer avec ses généraux, il imagina deux procédés de chiffrement. Le premier consistait à remplacer les lettres latines du message à crypter par des lettres grecques. Le second procédé est expliqué par Suétone dans son ouvrage *Les vies des douze César* écrit en 121 après Jésus-Christ. La technique en est particulièrement simple puisqu'il suffit de procéder à une permutation circulaire des lettres de l'alphabet en remplaçant chaque lettre par celle qui est située trois rangs plus loin : A est remplacé par D, B par E, C par F et ainsi de suite.

ANNEXE 2 : TEXTE RETROUVE SUR LE BUREAU DE LA VICTIME

LRILAM ! WBRD YBREQBWD MR ORY ! MHILD YBRYLD ELD MWWLLD TL ILEQLIEQLD, WBYIL HMYPLWEL LDY LWKPW ILEBUHLWDLL. CM UBCLERCL LDY HILYL M DROPI CM TLIWPLIL OMYYLIPL TL YLDYD LW CMOBIMYBPIL HBRI WBRD MDDRILI TL C'MODLWEL T'LKKLYD DLEBWTMPILD, EL FRP WBRD HLIULYYIM TL CM YLDYLI DRI TLD EBOMNLD. LY LWDRPYL … WBRD HBRIIBWD ILEBCYLI CLD KIRPYD TL WBD LKKBIYD. DMWD BROCPLI YBRYLD ELD GPLD FRL WBRD HBRIIBWD DMRGLI YLCD TLD DRHLI-QLIBD !