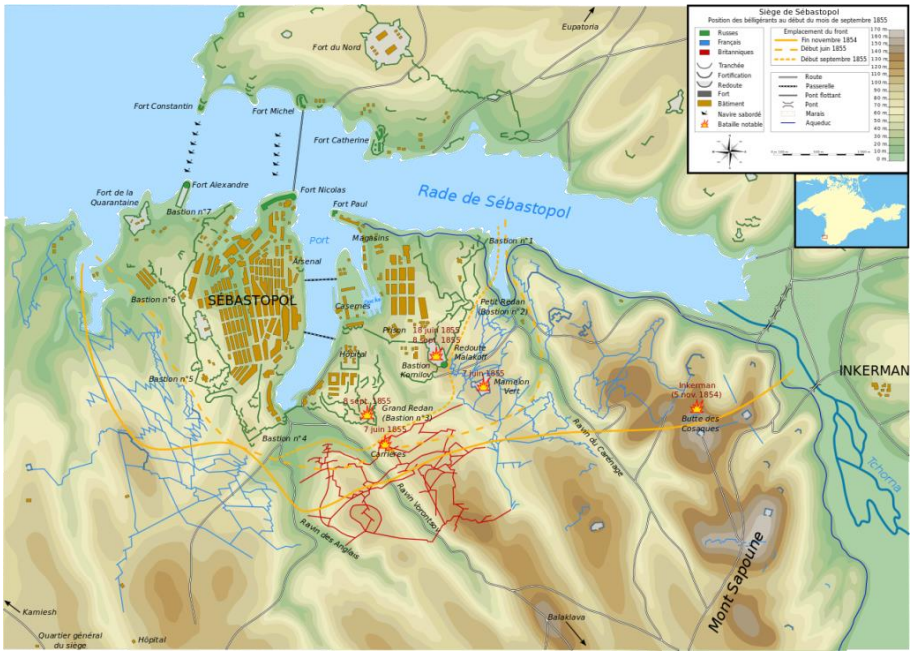
LOGICIEL DE CHIFFREMENT

CONTEXTE

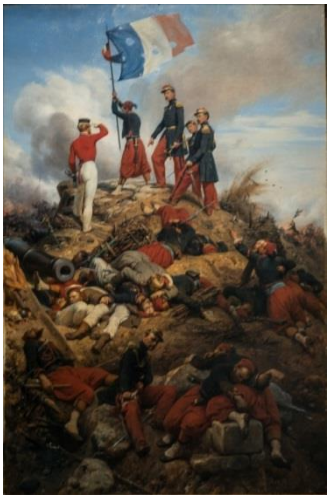
La guerre de Crimée opposa de 1853 à 1856 l'Empire russe à une coalition formée de l'Empire ottoman, de la France, du Royaume-Uni et du royaume de Sardaigne. Provoqué par l'expansionnisme russe et la crainte d'un effondrement de l'Empire ottoman, le conflit se déroula essentiellement en Crimée autour de la base navale de Sébastopol. Il s'acheva par la défaite de la Russie, entérinée par le traité de Paris de 1856.

Le siège de Sébastopol est l'épisode principal de la guerre de Crimée. Pénible et meurtrier, il dura onze mois, du 9 octobre 1854 au 11 septembre 1855.



En septembre 1854, les troupes alliées atteignirent la Crimée et commencèrent le siège de Sébastopol, port d'attache de la Marine impériale russe sur la mer Noire dont la flotte menaçait la Méditerranée. A partir du mois d'octobre, les troupes commencèrent la construction d'une ligne de siège au sud de Sébastopol. Les troupes creusèrent des abris, des tranchées et installèrent leurs canons.

Presque un an après, le 8 septembre 1855, les Français parviennent à s'emparer de la position fortifiée de Malakoff grâce à un assaut parfaitement coordonné. La forteresse devient alors intenable et les Russes l'évacuent après avoir détruit ses fortifications. Trois jours plus tard, la ville de Sébastopol finit par se rendre.



L'assaut du 8 septembre

La 1re division du général Mac Mahon est déployée contre Malakoff. Vers 8 h, les sapeurs français font exploser trois mines contenant chacune 500 kilogrammes d'explosifs entre les tranchées et Malakoff pour détruire les sapes russes. À midi précise, le pilonnage s'interrompt soudainement et au son des clairons et des tambours, le 1er régiment de zouaves et le 7ème régiment d'infanterie s'élancent à l'assaut de Malakoff.

LE BESOIN

Le commandant en chef de l'armée française, le général Pélissier, souhaite mettre en place un système de communication chiffré entre l'Etat major et les commandants des divisions françaises. En effet, les messages, étant la plus part du temps transmis par courriers se déplaçant à pied entre l'Etat major et les postes de commandement divisionnaires, ceux-ci étaient à la merci d'être interceptés par une patrouille de reconnaissance russe.



Les activités de renseignement relèvent, au ministère de la Guerre, de sa deuxième section, celle de la « Statistique militaire et des Travaux régimentaires » créée en 1826. Ce service est installé, au fort d'Aubervilliers, à Paris, sous le commandement du Lieutenant Colonel Auguste-Laurent Michel.

Vous êtes un jeune officier de la section de la « Statistique militaire » détaché à l'Etat major du général Pélissier.

Celui-ci, souhaite transmettre les instructions d'attaque à la position fortifiée de Malakoff, à destination du Général Mac Mahon. Le logiciel de chiffrement à mettre en œuvre devra alors permettre de chiffrer, puis de déchiffrer, à tour de rôle, les phrases suivantes :

Texte CHIFFRE	Texte DECHIFFRE
Ncufabm Nri KdctlZ	**General Mac Mahon**
Hpgskfnc np ethq fh ethq d khapW	**Pilonage le huit de huit a midi**
Dqqdsoh Nbkkqurr b khah	**Attaque Malakoff a midi**
Ibb Cfckhcf Fcn Vqorwpu	**Par Premier Reg Zouaves**
Hu Uphspcnh Fck CunfkuhacpZ	**Et Septieme Reg Infanterie**
Qpkgc Nfucfbk HckpyypcbV	**Signe General Pelissier**

LEXIQUE

- Aimable Jean Jacques PELISSIER, duc de Malakoff est un militaire français né le 6 novembre 1794 à Maromme et mort à Alger le 22 mai 1864. Appelé en Crimée pour y prendre le commandement en chef des troupes françaises, il est fait maréchal de France après la chute de Sébastopol le 12 septembre 1855.
- Patrice de MAC MAHON, comte de Mac Mahon, 1er duc de Magenta, né le 13 juin 1808 au château de Sully (Saône-et-Loire) et mort le 17 octobre 1893 à Montcresson (Loiret). Commande la 1ère division d'infanterie du 2ème corps de l'armée d'Orient et, en septembre 1855, il mène avec succès, pendant le siège de Sébastopol, l'attaque sur les ouvrages fortifiés de Malakoff.

DEFINITIONS

Sources :

Cours « Cybersécurité – Aspects techniques. H. GIMENEZ
WIKIPEDIA (https://fr.wikipedia.org)

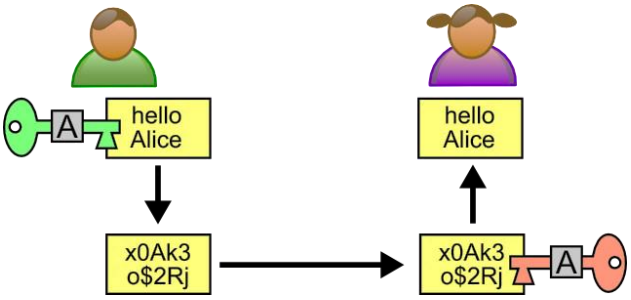
LE CRYPTAGE (OU CHIFFREMENT)

Le cryptage va prendre des données et va utiliser un algorithme pour les rendre INCOMPREHENSIBLES. Cela va permettre d'ENVOYER des données, et que seuls ceux qui sont en possession de la CLE DE CHIFFREMENT pourront lire ».

LE CHIFFREMENT A CLE SYMETRIQUE

Si l'on souhaite envoyer des informations, sans que des tiers non autorisés puissent les lire, il faudra alors les crypter (ou « chiffrer »). Mais encore faut-il que le destinataire du message puisse le lire : il faudra alors lui donner le moyen de les déchiffrer. Le principe est simple :

- On utilise un logiciel (algorithme) pour chiffrer le message.
- On communique au destinataire l'algorithme pour le décrypter, et peut donc lire le message.
- Une SEULE CLE est utilisée pour coder et décoder les données.



Si l'on envoie des messages différents à plusieurs personnes, celles qui seront en possession de la clé de cryptage pourront également lire des messages qui ne leurs sont pas destinés. Donc, pour communiquer en toute sécurité :

- Il faudra échanger autant de clés que l'on a d'interlocuteurs ;
- On devra trouver un moyen de communication sûr pour faire parvenir cette clé aux destinataires

Ce sont les 2 principaux inconvénients de ce type de cryptage. Par contre, les algorithmes à chiffrement symétriques ont l'avantage d'être rapides.

On peut citer les algorithmes de chiffrement symétriques suivants :

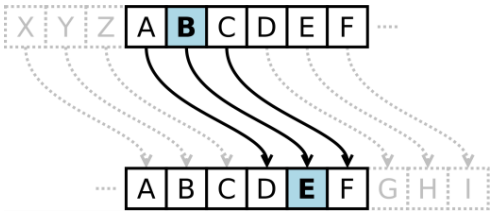
- **Le « Data Encryption Standard »** (DES) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable. Quand il est encore utilisé c'est généralement en Triple DES, ce qui ne fait rien pour améliorer ses performances.

- **L' « Advanced Encryption Standard »** ou AES (« norme de chiffrement avancé »), aussi connu sous le nom de « RIJNDAEL », est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il est actuellement le plus utilisé et le plus sûr

LE CHIFFREMENT PAR SUBSTITUTION POLYGRAMMIQUE.

Il s'agit d'une technique de chiffrement utilisée depuis bien longtemps, puisque le « chiffre de César » en est un cas particulier. Sans autre précision, elle désigne en général un chiffrement par substitution mono alphabétique, qui consiste à substituer dans un message chacune des lettres de l'alphabet par une autre (du même alphabet ou éventuellement d'un autre alphabet),

EX : le chiffre ou le code de César, est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes (ce qui explique le nom « chiffre de César »):



- Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet.
- Pour les dernières lettres (dans le cas d'un décalage à droite), on reprend au début. Par exemple avec un décalage de 3 vers la droite, A est remplacé par D, B devient E, et ainsi jusqu'à W qui devient Z, puis X devient A etc. Il s'agit d'une permutation circulaire de l'alphabet.
- La longueur du décalage, 3 dans l'exemple évoqué, constitue la clé du chiffrement qu'il suffit de transmettre au destinataire — s'il sait déjà qu'il s'agit d'un chiffrement de César — pour que celui-ci puisse déchiffrer le message. Dans le cas de l'alphabet latin, le chiffre de César n'a que 26 clés possibles (y compris la clé nulle, qui ne modifie pas le texte).

L'ALGORITHME DE CHIFFREMENT A DEVELOPPER

L'algorithme sera basé sur une méthode de chiffrement symétrique par substitution polygrammique.

- Cet algorithme remplace chaque paire de lettres du texte clair par une autre paire.
- Pour cela, il utilise une matrice carrée d'ordre cinq (5 lignes et 5 colonnes), construite à partir d'une clé convenue à l'avance, et qui contient toutes les lettres de l'alphabet, à l'exception d'une (souvent le J, confondue avec le I).

ELEMENTS TECHNIQUES

Des PAIRES de lettres sont cryptées, au lieu de lettres UNIQUES comme dans le cas d'un chiffre de substitution simple. Une grille 5 × 5 avec les lettres de l'alphabet sert de clé pour crypter le texte en clair. Sur les 26 lettres de l'alphabet, on en omet une, généralement 'J'. Dans ce cas, si le message à chiffrer contient un 'J' alors il sera remplacé par 'I'.

1) **Générer la GRILLE (5*5) à partir de la CLE :** `char[,] grille = new char[5,5];`

   - Si la CLE n'est pas fournie, prendre « CIPHER ».
   - Supprimer tous les caractères 'J' qui pourraient se trouver dans la CLE (cf. méthode `Replace` de la classe `string`).

\	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	K
2	L	M	N	O	P
3	Q	R	S	T	U
4	V	W	X	Y	Z

SUGGESTION : travailler sur une chaîne (`string`) qui servira ensuite à charger la grille (« chaîne de travail »). Par exemple, si la valeur de la CLE est "MONARCHY", la chaîne de travail initiale sera : "MONARCHY" + "ABCDEFGHIKLMNOPQRSTUVWXYZ" (=contenu initial de la grille).

\	0	1	2	3	4
0	M	O	N	A	R
1	C	H	Y	B	D
2	E	F	G	I	K
3	L	P	Q	S	T
4	U	V	W	Y	Z

   - Pour chaque caractère (25 en tout) correspondant au contenu initial de la grille par défaut ("ABCDEFGHIKLMNOPQRSTUVWXYZ"), rechercher les RANGS dans la chaîne de travail.
     EX : Pour 'A' (ligne 0, colonne 0) vs "**MONARCHY**ABCDEFGHIKLMNOPQRSTUVWXYZ" on trouve les rangs {3, 8}.
   - Supprimer alors de la chaîne de travail tous les doublons de 'A' (ici le doublon situé au rang 8).
     Soit : "**MONARCHY**BCDEFGHIKLMNOPQRSTUVWXYZ"
   - Une fois les 25 caractères traités, on aboutit à la dernière version de la chaîne de travail : "**MONARCHYBDEFGIKLPQSTUVWYZ**". Il s'agit alors de remplir la grille avec les 25 premiers caractères.

2) **Supprimer dans le MESSAGE à traiter (EX : `"Hello World"`) les caractères n'appartenant pas à l'alphabet.**

3) **Si le nombre de lettres du message est impaire, on en ajoute un 'X'.** Rappel : un nombre est PAIRE si le reste de la division entière par 2 est égal à zéro. EX : "INSTRUMENTS" --> **'IN' 'ST' 'RU' 'ME' 'NT' 'SZ'**

Méthodes utiles de la classe « `string` »

```
IsNullOrEmpty()
ToUpper()
Replace()
Substring()
IndexOf()
Remove()
```

Méthodes utiles de la classe « `char` »

```
IsLetter()
```

4) **On applique les REGLES DE SUBSTITUTION (chiffrement)**

Le message à chiffrer est découpé en PAIRES de 2 caractères (dans la boucle `for` penser à incrémenter le compteur par 2).

a) Pour chaque PAIRE de caractères (caractères de rang « i » et « i+1 ») on calcule leurs coordonnées correspondantes dans la grille.

\	0	1	2	3	4
0	M	O	N	A	R
1	C	H	Y	B	D
2	E	F	G	I	K
3	L	P	Q	S	T
4	U	V	W	Y	Z

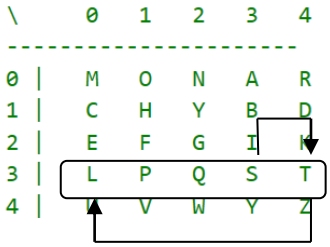
EX : 'M' et 'E'.

Pour 'M' => {ligne1 = 0; colonne1 = 0} et pour 'E' => {ligne2 = 2 ; colonne2 = 0}.
RAPPEL : si c'est un 'J' alors on recherche la position de 'I' qui le remplace.

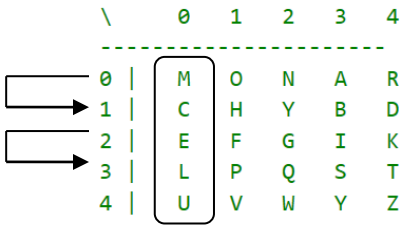
b) En fonction des coordonnées des 2 caractères, on applique la SUBSTITUTION. Pour cela, on peut constituer (par des concaténations successives) au fur et à mesure que l'on obtient CHAQUE PAIRE DE SUBSTITUTION, un objet **`string`** qui représentera le message codé.

REGLE 1 : si les 2 caractères se trouvent sur la MEME LIGNE et sur la MEME COLONNE (= les 2 caractères sont égaux), alors on retourne 2 fois le caractère situé à la (ligne + 1) et à la (colonne + 1).

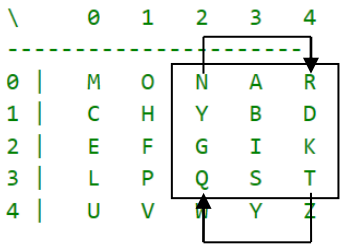
REGLE 2 : si les 2 caractères se trouvent sur la MÊME LIGNE, les remplacer par ceux se trouvant immédiatement à leur droite (en bouclant sur la gauche si le bord de la grille est atteint). EX : soit la paire "ST"; on la substitue par 'S' -> 'T' et 'T' -> 'L'



REGLE 3 : si les 2 caractères apparaissent sur la MÊME COLONNE, les remplacer par ceux qui sont juste en dessous (en bouclant sur le haut si le bord de la grille est atteint). EX : soit la paire "ME" ; on la substitue par 'M' -> 'C' et 'E' -> 'L'



REGLE 4 : si aucune des règles ci-dessus n'est vraie: formez un RECTANGLE avec les deux lettres et prenez les lettres dans le coin horizontal opposé du rectangle. EX: soit la paire "NT ; on la substitue par 'N' -> 'R' et 'T' -> 'Q'



REMARQUES

```
// Construire une chaîne à partir d'un tableau de caractères.
char[] letters = { 'A', 'B', 'C' };
string alphabet = new string(letters);
```

Pour DECHIFFRER un message, les règles précédentes sont identiques, sauf que pour :

- REGLE 1 : on retourne 2 fois le caractère situé à la (ligne - 1) et à la (colonne - 1)
- REGLE 2 : si les 2 caractères se trouvent sur la MEME LIGNE, les remplacer par ceux se trouvant immédiatement sur leur GAUCHE.
- REGLE 3 : si les 2 caractères se trouvent sur la MEME COLONNE, les remplacer par celles se trouvant juste au DESSUS.
- REGLE 4 : sinon, remplacer les caractères par ceux se trouvant sur la même ligne, mais dans le coin opposé du rectangle défini par la paire originale, en commençant par la lettre sur la même ligne que la première lettre à déchiffrer.

On fournit deux fonctions « utilitaires » :

```
// TEST DE DEPASSEMENT
// Permet de traiter les "bouclements" en cas de dépassement de rang en application des règles 1 à 3.
// ON FOURNIT le rang (ligne ou colonne) et la grille (pour avoir son nombre de lignes ou de colonnes)
// RETOURNE :
//      * En cas de codage, si dépassement à "droite" : zéro
//      * En cas de décodage, si c'était le résultat d'un bouclage alors rang == -1; on retourne le rang de
//        la dernière ligne ou colonne.
//      * Sinon, on retourne le même rang.
private static int TestDeDepassement(int rang, char[,] grille)
{
      if (rang == grille.GetLength(0))
          return 0;
      else
      {
          // Si index == -1 c'est que l'on avait bouclé
          if (rang == -1)
              rang = grille.GetLength(0) + rang;

          return rang;
      }
}
```

Précédemment, pour chaque paire de caractères du message (cf. boucle « for », on a concaténé au résultat la PAIRE DE SUBSTITUTION correspondante. La fonction suivante permet de « retoucher » la chaîne ainsi produite avant de la retourner à l'utilisateur :

```
// ON RETOUCHE" LA CHAÎNE TRAITÉE (chiffrée ou déchiffrée) :
//   * On compare caractères de même rang entre cette chaîne et le message d'origine
//   * Si le caractère d'origine 'i' n'appartient pas à l'alphabet, on l'ajoute tel quel
//   * Si le caractère d'origine 'i' était en minuscules alors on fait pareil dans la chaîne traitée
// PARAMETRES :
//   * input : le message à traiter
//   * output : résultat du traitement effectué pour chaque paire, en concaténant la paire de substitution correspondante.
/*
EX : Sans cette fonction,
     * Si le message en clair était "Hello World", on afficherait un message codé : "ECTTQVVGMB" au
       lieu de "Ecttq Vvgmb"
     * Si le message chiffré était "ECTTQVVGMB", on afficherait un message en clair : "HELLOWORLD" au
       lieu de "Hello World"
*/
private static string RetoucherChaine(string input, string output)
{
    StringBuilder aRetourner = new StringBuilder(output);

    // Parcours autant de fois qu'il y a de caractères dans le message à traiter
    for (int i = 0; i < input.Length; ++i)
    {
        // Le caractère n'appartient pas à l'alphabet. On l'ajoute à la chaîne traitée, au rang 'i'
        if (!char.IsLetter(input[i]))
            aRetourner = aRetourner.Insert(i, input[i].ToString());

         // Si le caractère 'i' du message d'origine est en minuscule, on le remplace par la version
         // minuscule du caractère de même rang dans la chaîne traitée.
         if (char.IsLower(input[i]))
             aRetourner[i] = char.ToLower(aRetourner[i]);
     }

     return aRetourner.ToString();
}
```

Fonction Main() :

```
         static void Main(string[] args)
        {
            // message en clair:"Hello World"; message chiffré :"Ecttq Vvgmb
            string texte = "Hello World";
            // string texte = "General Mac Mahon";
            // string texte = "Pilonage le huit de huit a midi";
            // string texte = "Attaque Malakoff a midi";
            // string texte = "Par Premier Reg Zouaves";
            // string texte = "Et Septieme Reg Infanterie";
            // string texte = "Signe General Pelissier";

            string texte_chiffre = Chiffrer(text, "cipher");            // CLE = “cipher”
            string texte_dechiffre = Dechiffrer(cipherText, "cipher");  // CLE = “cipher”

            Console.WriteLine(texte_chiffre);
            Console.WriteLine(texte_dechiffre);
            Console.ReadKey();
        }
```