Cryptage d'un message

Le travail peut être réalisé en binôme, il est déposé dans le répertoire suivant  sous Spiral



Pour le réaliser, vous devez maîtriser le langage C#. Ce tp s’adresse aux étudiants **issus d’un IUT ou d’un BTS informatique**.

La transposition en colonnes est une manière simple et relativement efficace de chiffrer un message. Cette méthode fonctionne avec une **clef connue de l'émetteur ainsi que du récepteur,** il s'agit donc de la même clef que ce soit pour chiffrer ou déchiffrer le texte.

Exemple : texte à crypter = « L’istil devient uné école polytechnique »

Clé : **ISTIL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I** | **S** | **T** | **I** | **L** |
| **0** | **3** | **4** | **1** | **2** |
| **L** | **‘** | **I** | **S** | **T** |
| **I** |  | **D** | **E** | **V** |
| **I** | **E** | **N** | **T** |  |
| **U** | **N** | **E** |  | **E** |
| **C** | **O** | **L** | **E** |  |
| **P** | **O** | **L** | **Y** | **T** |
| **E** | **C** | **H** | **N** | **I** |
| **Q** | **U** | **E** |  |  |
|  |  |  |  |  |

Texte chiffré : « LIIUCPEQ SET EYN TV E TI ‘ ENOOCU IDNELLHE »

**Principe :** un mot clé secret est utilisé pour dériver une séquence de chiffres commençant à 0 et finissant au nombre de lettres composant le mot clé. Cette séquence est obtenue en numérotant les lettres du mot clé en partant de la gauche vers la droite et en donnant l’ordre d’apparition dans l’alphabet. Une fois que la séquence de transposition est obtenue, on chiffre en écrivant d’abord le message par lignes dans un rectangle (puis on lit le texte par colonnes en suivant l’ordre déterminé par la séquence.

Nous allons prendre pour l'exemple la clef : **MIAGEISTIL** qui contient **5** caractères (c'est important à savoir pour la suite). Nous allons maintenant convertir la clef en suite logique de chiffres :

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | I | A | G | E | I | S | T | I | L |
| 7 | 3 | 0 | 2 | 1 | 4 | 8 | 9 | 5 | 6 |

Pourquoi ? **A** est la première lettre de l'alphabet présente dans la clé, elle vaut donc **0**, la deuxième étant **E**, celle-ci vaut **1**, puis **G** = **2**, etc...  
Vous remarquerez qu'il y a trois I dans la clé, dans ce type de cas, on va lire de la gauche vers la droite, ainsi le **I**  à gauche vaut **3** et celui le plus à droite **5**.

Une fois que la suite de chiffres est déterminée, nous allons générer une colonne. Sachant que le message que l'on souhaite chiffrer est : "Bienvenue à l’ISTIL, dans le monde des ingénieurs" :

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | I | A | G | E | I | S | T | I | L |
| 7 | 3 | 0 | 2 | 1 | 4 | 8 | 9 | 5 | 6 |
| B | i | e | n | v | e | n | u | e |  |
| à | l | ‘ | I | S | T | I | L | , |  |
| d | a | n | s |  | l | e |  | m | o |
| n | d | e |  | d | e | s |  | i | n |
| g | é | n | i | e | u | r | s | @ | @ |

Comme ci-dessus, il faut toujours compléter la dernière ligne par une lettre comme @

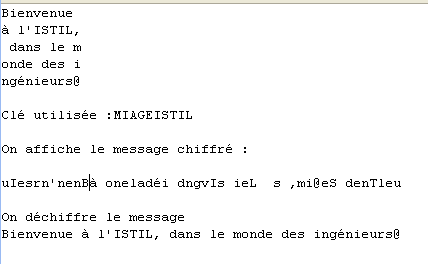
Pour crypter le code, nous allons prendre successivement la colonne du numéro 0, 1, 2 puis 3, etc...  
Ce qui donne :  
  
**e’nen vs de nIs i iladé eTleu e,mi@ on@ Bàdng nIesr uL s**

**Déchiffrer**

Pour commencer, nous devons connaître trois choses, la clef (fournie par l'émetteur), la longueur de clef (ici 10), ainsi que la longueur du texte (30). Une fois toutes ces informations réunies, nous allons effectuer un simple calcul permettant de trouver le nombre de lignes ainsi que le nombre de colonnes :  
  
longueur de texte = longueur de clef \* ?  
  
Donc avec notre texte, cela donne :  
  
48 = 10 \* 5 -2  
  
Nous aurons donc 5 lignes de 10 caractères. Nous pouvons donc générer le tableau :  
  
  
Pour remplir le tableau, comme nous savons qu'il faut 5 caractères par colonne, nous plaçons les trois premières à savoir e’nen sous le 0 puis vS de sous le 1, puis iladé sous le 3, etc...

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | I | A | G | E | I | S | T | I | L |
| 7 | 3 | 0 | 2 | 1 | 4 | 8 | 9 | 5 | 6 |
| B | i | e | n | v | e | n | u | e |  |
| à | l | ‘ | I | S | T | I | L | , |  |
| d | a | n | s |  | l | e |  | m | o |
| n | d | e |  | d | e | s |  | i | n |
| g | é | n | i | e | u | r | s | @ | @ |

Exemple :



**Travail à faire**

Réalisez une application interactive qui permette le chiffrement et le déchiffrement d’un message avec une clé de votre choix