**Exercice 1 : (décalage)**

On rappelle qu’on a la numérotation des lettres de l’alphabet suivante :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 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 |

1. Coder le message « la rencontre est prévue à la cafétéria » à l’aide du chiffrement par décalage et de la clé K = 5.

2. Décoder le message « RGNEIDVGPEWXTRAPHHXFJT » sachant qu’il a été créé par un chiffrement par décalage.

**Solution :**

1. Pour trouver le texte chiffré on applique la formule suivante :

**Lettre chiffrée=lettre claire+k mod 26**

On obtient le message chiffré suivant :

**« qfwjshtsywjjxyuwjazjfqfhfkjyjwnf »**

1. Pour déchiffrer le message « **RGNEIDVGPEWXTRAPHHXFJT**», on peut tester toutes les valeurs possibles de la clé jusqu'à arriver au bon message, nous avons 26 possibilités.

**Exercice 2 :** (analyse fréquentielle)

L’analyse des fréquences d’apparition des lettres dans un message codé montre que ceux sont les lettres K et O les plus fréquentes dans ce message. Dans un texte en français les lettres les plus fréquentes sont le A (8.4%) et le E (17.26%). Sachant que le message est en français, codé en utilisant le chiffrement par décalage sur les 26 lettres de l’alphabet, déterminer la clef et déchiffrer le début du message :

**SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC**

**Solution :**

En se basant sur l’analyse fréquentielle du message chiffré et en comparant avec les lettres les plus fréquentes en langue française on déduit que la lettre K correspond à la lettre A après le chiffrement et la lettre E correspond à la lettre E. Donc la clé du chiffrement *k*=10.

On applique la formule suivante pour trouver le texte clair :

Lettre claire = Lettre chiffrée –*k* mod 26.

On obtient le texte clair suivant :

**« ILENVOYADANSLALIGURIEACHETERDESSOLDATS »**

**Exercice 3 :** (substitution)

1- Coder le message « la rencontre est prévue à la cafétéria » à l’aide du chiffrement par substitution et de la clé suivante :

a b c d e f g h i j k l m n o p q r s t u v w x y z

X N Y A H P O G Z Q W B T S F L R C V M U E K J D I

1. Est-il possible de décoder le message « YHVMQUVMH » codé par un chiffrement par substitution sans connaître la clé. Décoder ce message sachant qu’il a été créé avec la clé précédente.

**Solution :**

1. On remplace chaque lettre dans le message claire par la lettre qui lui correspond selon la clé du chiffrement.

**« BXCHSYFSMCH HVMLCHEUHXBXYXPHMHCZX »**

1. Non, ce n'est pas possible que si le texte est long en se basant sur l'analyse fréquentielle.

En connaissant la clé, le déchiffrement est immédiat. On remplace chaque lettre dans le message chiffré par la lettre qui lui correspond selon la clé du chiffrement. Donc le message chiffré **« YHVMQUVMH »** correspond au message clair : **« CESTJUSTE »**

**Exercice 4 :** (Vigenère)

1. Coder le message « la rencontre est prévue à la cafétéria » à l’aide de la méthode de Vigenère et du mot clé POULE.

2. Est-il possible de décoder le message « DSJWPHYRSSUHPAJXVQV » codé par un chiffrement de Vigenère sans connaître la clé. Décoder ce message sachant qu’il a été créé à l’aide du mot clé BORDEAUX.

**Solution :**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 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 |

1. Le mot clé POULE est de longueur 5, donc on divise le texte en blocs de 5 lettres et on calcule pour chaque bloc le texte chiffré on utilisant les clés (n1, n2, n3, n4, n5)= (**15,14,20,11,4**). La formule utilisée pour le chiffrement est :

**Lettre chiffrée=lettre claire+ni mod 26**

Exemple :

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **l** | **a** | **r** | **e** | **n** | **c** | **o** | **n** | **t** | **r** |
| **11+15** | **0+14** | **17+20** | **4+11** | **13+4** | **2+15** | **14+14** | **13+20** | **19+11** | **17+4** |
| **a** | **o** | **l** | **p** | **r** | **r** | **c** | **h** | **e** | **v** |

Donc à partir du message clair :

**« laren contr eestp révue àlaca fétér iat »**

On obtient le texte chiffré suivant :

**«  aolpr rchev tsmet gspfi pzune usnpv xon »**

1. Non, ce n'est pas possible que si le texte est long, on commençant par calculer la taille de la clé. Les techniques sans clé les plus courantes utilisent des méthodes statistiques qui permettent de retrouver la longueur de la clé, puis une analyse des fréquences d’apparition des lettres permet de retrouver la clé.

A partir du message **« DSJWPHYR SSUHPAJX VQV »** chiffré avec le mot clé BORDEAUX qui correspond aux clés (n1,n2,n3,n4,n5,n6,n7,n8)=(1,14,17,3,4,0,20,23),on applique la formule du déchiffrement suivante :

**Lettre claire = Lettre chiffrée –ni mod 26**

Exemple :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **d** | **s** | **j** | **w** | **p** | **h** | **y** | **r** |
| **3-1** | **18-14** | **9-17** | **22-3** | **15-4** | **7-0** | **24-20** | **17-23** |
| **c** | **e** | **s** | **t** | **l** | **h** | **e** | **u** |

On obtient le texte clair suivant : « **CESTLHEUREDELAPAUCE »**