Le décryptage du message trouvé chez Durand.

« JAANC NUJ
NUUNE JCXDC OJRAN AJCNA
OJRBU NWNLN BBJRA N
SNLXV YCNBD ACXR
SNO »

Le message a été crypté avec le code de César.

1 -Recherche de la clé.

L'analyse des fréquences montre que le *N* est la lettre la plus représentée.

Méthode 1 : La recherche des fréquences peut se faire avec la fonction « chercher remplacer » du traitement de texte.

Méthode 2 : On peut aussi réaliser un programme avec algobox : on entre le message, on fixe une lettre, le programme affiche la fréquence d'apparition de la lettre dans le message. Voir le fichier message_cesar_frequence.alg.

```
1 VARIABLES
2 longueur EST_DU_TYPE NOMBRE
3 k EST_DU_TYPE NOMBRE
4 lettre EST_DU_TYPE CHAINE
5 compteur EST_DU_TYPE NOMBRE
6 freq EST_DU_TYPE NOMBRE
7 message EST_DU_TYPE CHAINE
8 DEBUT_ALGORITHME
9 LIRE message
10 longueur PREND_LA_VALEUR message.length
11 compteur PREND_LA_VALEUR 0
12 LIRE lettre
13 POUR k ALLANT_DE 0 A longueur-1
14 DEBUT_POUR
15 SI (lettre==message.substr(k,1)) ALORS
16 DEBUT_SI
17 compteur PREND_LA_VALEUR compteur+1
18 FIN_SI
19 FIN_POUR
20 AFFICHER "Fréquence d'apparition du "
21 AFFICHER lettre
22 AFFICHER " est égale à : "
23 freq PREND_LA_VALEUR compteur/longueur
24 AFFICHER freq
25 FIN_ALGORITHME
```

Résultat : L'analyse des fréquences du message montre que *N* est la plus représentée.
On peut donc penser que le N du message codé est le E du message initial.
La clé est donc 9.

2- Le décryptage

On entre le message codé avec le nombre correspondant à la clé.

On ne considère que les caractères de *a* à *z* en minuscules. Les codes ASCII vont de 97 à 122.
Pour chaque lettre du message crypté, on extrait le code ASCII auquel on retranche la clé.
Seulement, si le code ASCII est inférieur strictement à 97, il faut repartir de 122.

Méthode 1 : Avec le tableur.
Voir le fichier decodage_cesar_tableur.ods

On utilise ici les fonctions « cod() » et car() » pour passer de lettre à ascii et inversement.
(ci-dessous extrait de grille d'après élèves)

clé de césar=	9					
message initial	j	a	a	n	c	n
code ascii du message initial	106	97	97	110	99	110
code ascii-clé césar	97	88	88	101	90	101
nouveau code ascii	97	114	114	101	116	101
lettre décodée	a	r	r	e	t	e

Méthode 2 :
Avec algobox, on utilise les fonctions length, substr, charCodeAt et String.fromCharCode
Voir le fichier message_cesar_decodage.alg.

```
1 VARIABLES
2 message EST_DU_TYPE CHAINE
3 longueur EST_DU_TYPE NOMBRE
4 k EST_DU_TYPE NOMBRE
5 lettre EST_DU_TYPE CHAINE
6 cle EST_DU_TYPE NOMBRE
7 nb EST_DU_TYPE NOMBRE
8 DEBUT_ALGORITHME
9 LIRE message
10 LIRE cle
11 longueur PREND_LA_VALEUR message.length
12 POUR k ALLANT_DE 0 A longueur-1
13 DEBUT_POUR
14 nb PREND_LA_VALEUR message.charCodeAt(k)
15 nb PREND_LA_VALEUR nb-cle
16 SI (nb<97) ALORS
17 DEBUT_SI
18 nb PREND_LA_VALEUR 26+nb
19 FIN_SI
20 lettre PREND_LA_VALEUR String.fromCharCode(nb)
```

```
21 AFFICHER lettre
22 FIN_POUR
24 FIN_ALGORITHME
```

3- le cryptage

Ici encore, il est possible de coder au tableur mais nous nous limitons à algobox.

On entre des mots avec la clé, le programme affiche le message crypté.
Voir le fichier message_cesar_codage.alg.
On ne considère que les caractères de *a* à *z* en minuscules. Les codes ASCII vont de 97 à 122.
Pour chaque lettre du message crypté, on extrait le code ASCII auquel on ajoute la clé.
Seulement, si le code ASCII est supérieur strictement à 122, il faut repartir de 97.

```
1 VARIABLES
2 message EST_DU_TYPE CHAINE
3 longueur EST_DU_TYPE NOMBRE
4 k EST_DU_TYPE NOMBRE
5 lettre EST_DU_TYPE CHAINE
6 cle EST_DU_TYPE NOMBRE
7 nb EST_DU_TYPE NOMBRE
8 DEBUT_ALGORITHME
9 LIRE message
10 LIRE cle
11 longueur PREND_LA_VALEUR message.length
12 POUR k ALLANT_DE 0 A longueur-1
13 DEBUT_POUR
14 nb PREND_LA_VALEUR message.charCodeAt(k)
15 nb PREND_LA_VALEUR nb+cle
16 SI (nb>122) ALORS
17 DEBUT_SI
18 nb PREND_LA_VALEUR nb-26
19 FIN_SI
20 lettre PREND_LA_VALEUR String.fromCharCode(nb)
21 AFFICHER lettre
22 FIN_POUR
23
24 FIN_ALGORITHME
```

4° Remarque

Il est intéressant de mettre en relation des groupes travaillant sur le Code de César d'une part et sur le code Vigenère d'autres parts et de leur faire comparer les fréquences des lettres que l'on obtient sur un même message. Le code de Vigenère permet d'obtenir un diagramme en bâtons beaucoup plus lissé.