Mathys Domergue

RT2 App

TD

Message chiffré

Pour déchiffrer le message avec le carré de Vignère, on calcule d'abbord l'indice de coïncicence, ce qui nous donne :

```
Pour une longueur de clé de 2, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 3, l'indice de coïncidence vaut 0.058
Pour une longueur de clé de 4, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 5, l'indice de coïncidence vaut 0.044
Pour une longueur de clé de 6, l'indice de coïncidence vaut 0.076
Pour une longueur de clé de 7, l'indice de coïncidence vaut 0.043
Pour une longueur de clé de 8, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 9, l'indice de coïncidence vaut 0.057
Pour une longueur de clé de 10, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 11, l'indice de coïncidence vaut 0.042
Pour une longueur de clé de 12, l'indice de coïncidence vaut 0.077
Pour une longueur de clé de 13, l'indice de coïncidence vaut 0.044
Pour une longueur de clé de 14, l'indice de coïncidence vaut 0.048
Pour une longueur de clé de 15, l'indice de coïncidence vaut 0.061
Pour une longueur de clé de 16, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 17, l'indice de coïncidence vaut 0.043
Pour une longueur de clé de 18, l'indice de coïncidence vaut 0.077
Pour une longueur de clé de 19, l'indice de coïncidence vaut 0.041
Pour une longueur de clé de 20, l'indice de coïncidence vaut 0.048
```

Maintenant que cela est fait, nous allons prendre l'indice de coïncidence le plus élévé dasn notre cas il est à 0.076. Avec cette info on peut savoir la taille de la clé qui est 6

Longueur de clé choisie :

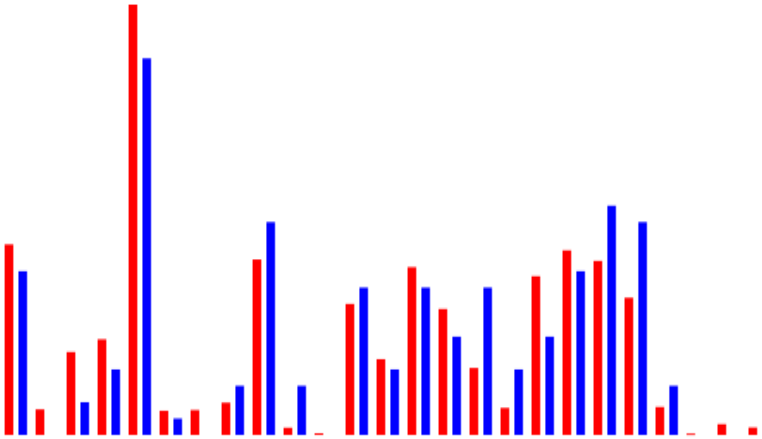
6

Rang de la lettre de la clé analysée :

1

Lancer l'analyse

- C +



Clé proposée :

C

Déchiffrer!

Longueur de clé choisie :

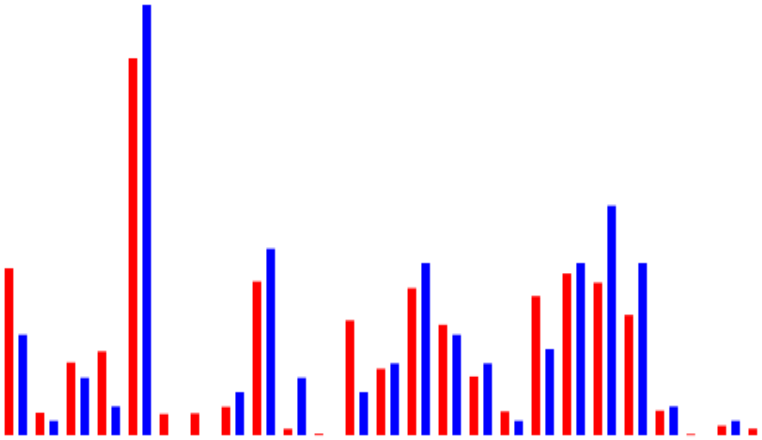
6

Rang de la lettre de la clé analysée :

2

Lancer l'analyse

- N +



Clé proposée :

CN

Déchiffrer!

Longueur de clé choisie :

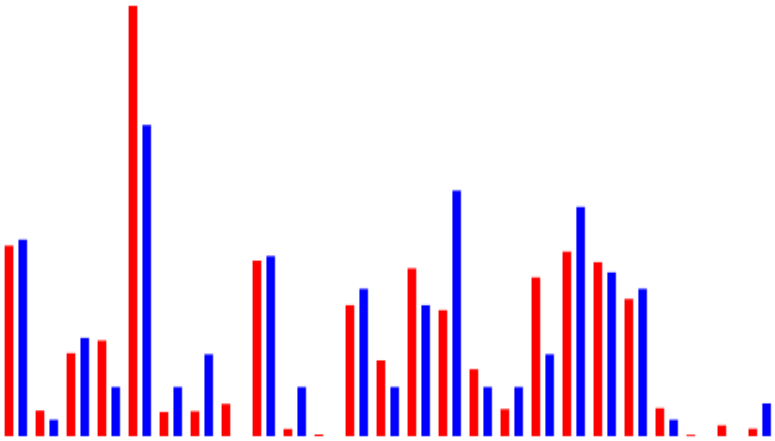
6

Rang de la lettre de la clé analysée :

3

Lancer l'analyse

- U +



Clé proposée :

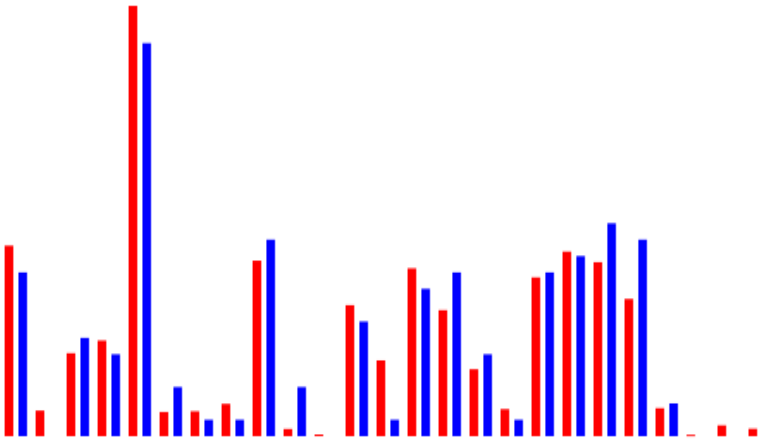
CNU

Déchiffrer!

Longueur de clé choisie :
6
Rang de la lettre de la clé analysée :
4

Lancer l'analyse

- G +



Clé proposée :

CNUG

Déchiffrer!

Longueur de clé choisie :

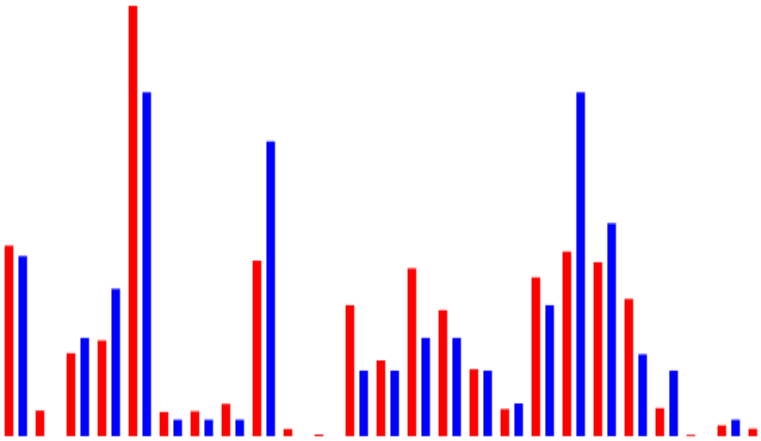
6

Rang de la lettre de la clé analysée :

5

Lancer l'analyse

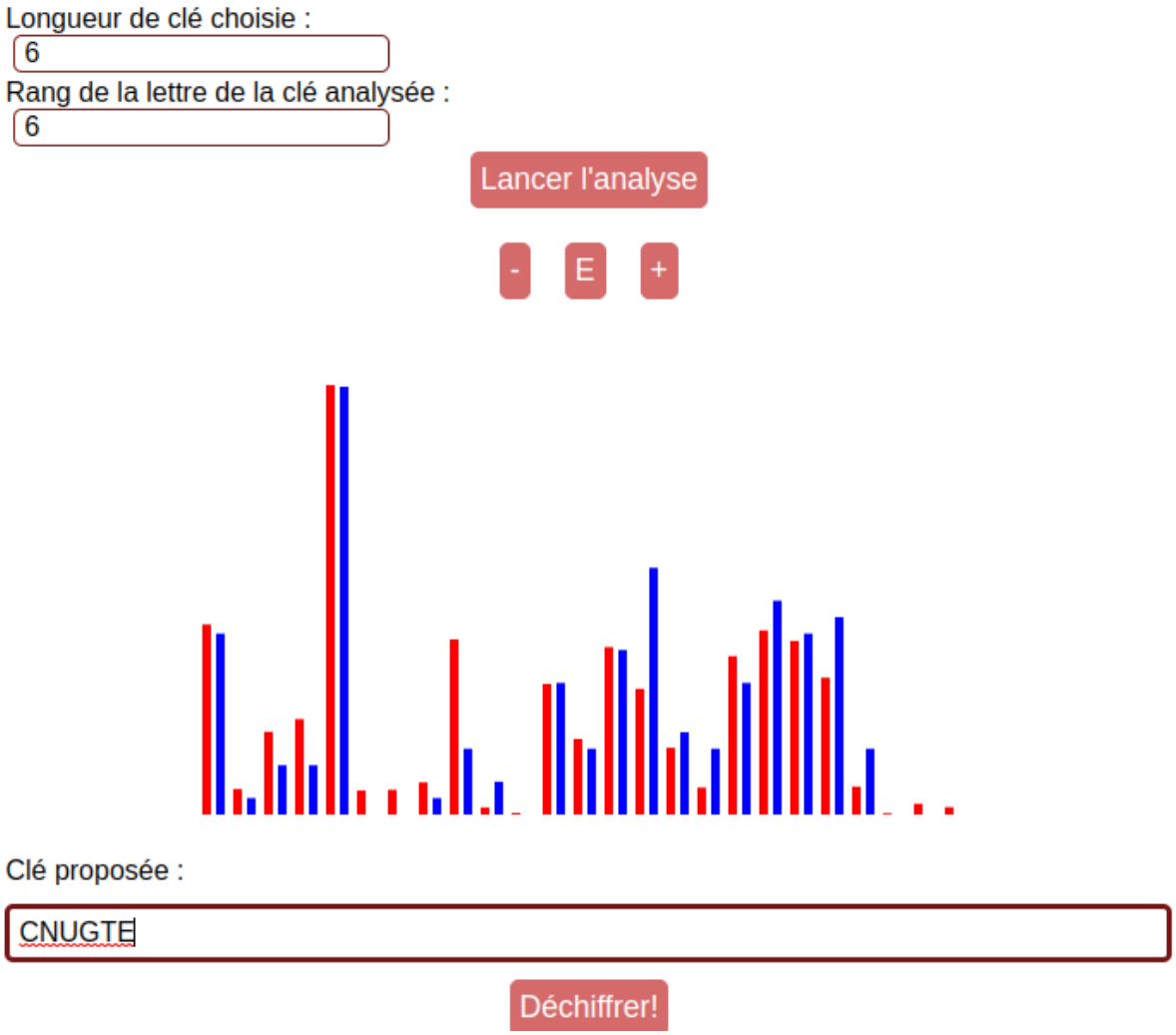
- T +



Clé proposée :

CNUGT

Déchiffrer!



Ce qui nous donne une clé qui vaut CNUGTE et le message donne:

```
FACE A CES MUTATIONS SANS DOUTE CONVIENT IL D’INVENTER D’INIMAGINABLES
NOUVEAUTÉS HORS LES CADRES DÉSUETS QUI FORMATENT ENCORE NOS CONDUITES ET
NOS PROJETS NOS INSTITUTIONS LUISENT D’UN ÉCLAT QUI RESSEMBLE AUJOURD’HUI A
CELUI DES CONSTELLATIONS DONT L’ASTROPHYSIQUE NOUS APPRIT J’ADIS QUELLES
ÉTAIENT MORTES DÉJÀ DEPUIS LONGTEMPS POURQUOI CES NOUVEAUTÉS NE SONT ELLES
POINT ADVENUES JE N’ACCUSE LES PHILOSOPHES DONT JE SUIS GENS QUI ONT POUR
METIER D’ANTICIPER LES A VOIR ET LES PRATIQUES AVENIR ET QUI ONT COMME MOI
CE ME SEMBLE FAILLI A LEUR TACHE EN GAGES DANS LA POLITIQUE AU JOUR LE JOUR
ILS NE VIRENT PAS VENIR LE CONTEMPORAIN SI J’AVAIS EU EN EFFET A CROQUER LE
PORTRAIT DES ADULTES DONT JE SUIS IL EUT ETE MOINS FLATTEUR JE VOUDRAIS
AVOIR DIX-HUIT ANS L’AGE DE PETITE POUCETTE ET DE PETIT POUCET PUIS QUE
TOUT EST A REFAIRE NON PUISQUE TOUT EST A FAIRE JE SOUHAITE QUE LA VIE ME
LAISSE ASSEZ DE TEMPS POUR Y TRAVAILLER ENCORE EN COMPAGNIE DE CES PETITS
AUXQUELS J’AI VOUE MA VIE PARCE QUE JE LES AI TOUJOURS RESPECTUEUSEMENT
AIMES
MICHEL SERRES PETITE POUCETTE
```

C'est haché

Pour déhacher les mots de passes, on peut utiliser la commande :

```
hashcat -m 0 -a 0 <hash> <wordlists>
```

Ce qui nous donne les mots de passes suivant:

```
ernesto:toroto
philippe:agnès
joao:braZiLL
admin:passwd
root:root
```