



TRAVAIL 2

Pif1006

Adam Lemire
Rémi Petiteau

UQTR
16 décembre 2016

Problèmes et difficultés rencontrées :

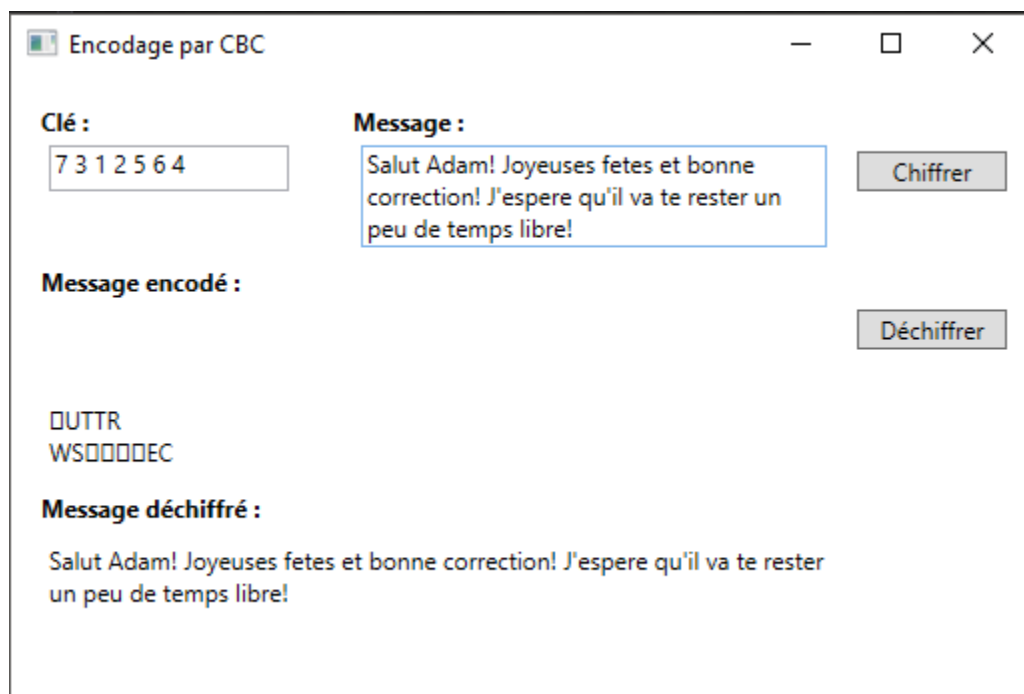
Il a fallu un certain temps pour comprendre une erreur : nous tentions d'effectuer des opérations sur des cases « nulles » créées lorsque le message n'emplissait pas totalement le tableau du message transposé. Pour résoudre ce problème, nous avons remplacé ces cases par des espaces vides, que nous effaçons au final. Nous émettons comme hypothèse qu'un message ne finit jamais par des caractères d'espacement.

Guide d'utilisation

Conditions :

- La clé doit être de la forme : 1 2 3 4 5 etc. comme spécifié dans l'énoncé du travail. Un nombre ne peut revenir 2 fois, et lorsque placés en ordre croissant, ils doivent suivre la forme : $i(0)=1$, $i(n)=n+1$.
- Le message ne doit contenir aucun accent. Les symboles « ! ? , ' » sont permis.
- Entrer la clé et le message dans les cases appropriées, puis utiliser les boutons pour effectuer l'opération désirée.

Exemple 1



The screenshot shows a window titled "Encodage par CBC" with the following fields and buttons:

- Clé :** A text box containing "7 3 1 2 5 6 4".
- Message :** A text box containing "Salut Adam! Joyeuses fetes et bonne correction! J'espere qu'il va te rester un peu de temps libre!".
- Chiffrer** button.
- Message encodé :** A text box containing "OUTTR" and "WSOEC" on separate lines.
- Déchiffrer** button.
- Message déchiffré :** A text box containing "Salut Adam! Joyeuses fetes et bonne correction! J'espere qu'il va te rester un peu de temps libre!".

Exemple 2

Encodage par CBC

Clé :

10 9 8 1 2 4 3 7 6 5

Message :

Message a tester avec une autre cle.
J'espere que tout va s'afficher
correctement et sans erreurs.

Chiffrer

Message encodé :

□□□EC□CUEAAQ□RVREED
N□ASBSSES□A??UR@]□□E□P RR?9

Déchiffrer

Message déchiffré :

Message a tester avec une autre cle. J'espere que tout va s'afficher
correctement et sans erreurs.

Exemple 3

Chiffrement et déchiffrement avec la même clé :

Encodage par CBC

Clé :

5 4 3 2 1

Message :

Message qui va surment mal se dechiffrer si on prend une cle differente pour le dechiffrement!

Chiffrer

Message encodé :

QUEAI

UIMS

Message déchiffré :

Message qui va surment mal se dechiffrer si on prend une cle differente pour le dechiffrement!

Déchiffrer

Déchiffrement avec une autre clé :

Encodage par CBC

Clé :

1 2 3 4 5

Message :

Message qui va surment mal se dechiffrer si on prend une cle differente pour le dechiffrement!

Chiffrer

Message encodé :

QUEAI

UIMS

Message déchiffré :

asseMuq eg av iemrusam tn es lihcedrerffo is erp nnu dnelc effid
tnereuop e el rihcedmerff !tne

Déchiffrer