

Université du Québec à Trois-Rivières



Université du Québec
à Trois-Rivières

TRAVAIL DE SESSION
PRÉSENTÉ
À

ADAM JOLY

COMME EXIGENCE PARTIELLE
DU COURS

MATHEMATIQUES POUR INFORMATICIEN II
CHIFFREMENT ET DECHIFFREMENT PAR CBC

FAIT PAR

ARMEL KUIBIA
JONATHAN KANYINDA
ISMAËL COULIBALY
JOSUE LUBAKI

TRAVAIL PRATIQUE 3

23 Décembre 2020

Table des matières

Présentation du Projet	3
Participation.....	3
Difficultés Rencontrées :	3
Guide utilisateur:	4

Présentation du Projet

Nom du Projet : EncryptionOperation

Langage Choisis : C#

Dépendance : NET Core 3.1.9

Participation

Les étudiants participants :

- ✓ Jordan Kuibia
- ✓ Jonathan Kanyinda
- ✓ Josue Lubaki
- ✓ Ismaël Coulibaly

Difficultés Rencontrées :

Comme difficulté majeure, le projet soumis ne gère pas les accents contenus dans le message. (Exemple : *ce cours est très intéressant*) ne sera pas chiffré à cause des accents sur le mot « très » et « intéressant ».

Pendant l'implémentation, la compréhension de conversion byte [] en String ou int en byte [] n'a pas été simple à saisir.

Guide utilisation:

Voici le menu principal. Il s'agit du premier affichage lorsqu'on lance l'exécution du programme.

```
MENU PRINCIPAL
```

Voici les Options disponibles :

- 1. Chiffrement
- 2. Dechiffrement
- 3. Chiffrement et Déchiffrement
- 4. Quitter

Sélectionner l'Option :

Example 1:

En sélectionnant l'option 3, on affiche les résultats des opérations de chiffrement et de déchiffrement simultanément, pour une clé et un même message.

```
Selectionner l'Option : 3
```

On entre le message comme suit : **“etudiant”**. On entre ensuite la clé **“7 1 4 5”**, en respectant un espace entre chaque chiffre. Le code affiche donc les résultats de la transposition, du chiffrement et du déchiffrement.

```

Veillez entrer un message : etudiant
Veillez entrer une clé (exemple :9 1 4 5 7) :
7 1 4 5
Votre message : etudiant
Voici le message transposé de "etudiant" :
    >>> taundtei

Message chiffré : 'F3]9M(A
Message déchiffré :
etudiant

```

Exemple 2:

Il est maintenant question d'effectuer la même procédure (en sélectionnant l'option 3) mais

```
Veuillez entrer un message : etudiant
Veuillez entrer une clé (exemple :9 1 4 5 7) :
4 2 1 3 9 7 6
Votre message : etudiant
Voici le message transposé de "etudiant" :
    >>> u t d etn a i

Message chiffré : &rR6siIaA

Message déchiffré :

etudiant
```

avec une clé d'une différente taille. On entre le même message, "**etudiant**".
La clé est "**4 2 1 3 9 7 6**".

Exemple 3:

Nous allons maintenant chiffrer un message avec une clé et déchiffrer le résultat avec une autre clé.

On sélectionne l'option 1 (chiffrement) et on rentre "**etudiant**" et "**2 9 5**" respectivement.

```
Selectionner l'Option : 1
Veuillez entrer un message : etudiant
Veuillez entrer une clé (exemple :9 1 4 5 7) :
2 9 5
Votre message : etudiant

Voici le message transposé de "etudiant" :
    >>> ednua tit

Message chiffré : 6R<I|a
```

Le message chiffré est "**6R<I|a**".

On sélectionne l'option 2 (déchiffrement), on entre "**6R<I|a**" avec "**9 4 6**" comme clé. Le résultat est le suivant :

```
Selectionner l'Option : 2
Veuillez entrer un message : 6R<I|a
Veuillez entrer une clé (exemple :9 1 4 5 7) :
9 4 6
Votre message : 6R<I|a

Message déchiffré :

5endu
```

Le message déchiffré est **“5endu”**.

On peut maintenant quitter le programme avec l'option 4 (quitter).

```

      ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■
      ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ MENU PRINCIPAL ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■
      ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■ ■■■■■■

Voici les Options disponibles :
    1. Chiffrement
    2. Dechiffrement
    3. Chiffrement et Déchiffrement
    4. Quitter

Selectionner l'Option : 4

```