Université de Québec à Rimouski
Campus de Lévis

Travail pratique #2 - Hachage MD5

Par
Fernand MATIGNON

Travail présenté à M. Martin Arsenault
Dans le cadre du cours Sécurité informatique
INF36207-MS

Mars2020

Application “Dictionnaire” :

Application développée en C# avec **Windows Form** *[b]* .

L’application dictionnaire *[1]* sert à générer des listes de “mot” selon une règle simple: *générer l’ensemble des combinaisons de mot possible selon les paramètres qui lui sont introduits*.
Les variables paramétrable sont :

- Les caractères permis dans le dictionnaire
- La longueure minimal
- La longueure maximal

L’application comporte plusieurs éléments:

- Une suite de “CheckBox”: pour créer rapidement une liste de caractères autorisés .
- Une “TextBox” : pour entrée une liste de caractères personnalisée (peut contenir tout type de caractères sauf séquence d'échappement type “tabulation”, “entrer”, etc…).
- Deux “**UpDownBox**”*[c]* : pour definire les valeur “longueure minimal” et “longueure maximal” (la longueure minimal ne peut pas être inférieure à 0 ni être supérieur à la longueure maximum)
- Un bouton de génération du dictionnaire.

Avant de commencer la génération l’application informe l’utilisateur de l’espace que va occuper le dictionnaire. *[2]*

Le bouton “Générer” laisse alors place à une barre de progression. *[3]*

Application “Hachage” :

Application développée en C# avec **Windows Form** *[b]*.

L’application hachage *[4]* sert à retrouver le mot de passe correspondant à un hash entrer par l’utilisateur, à l’aide d’un dictionnaire de mot.

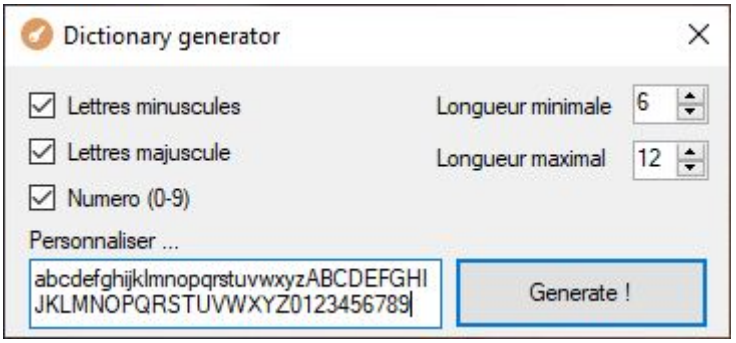
L’application comporte plusieurs éléments:

- Une “TextBox”: pour récupérer le hash de l’utilisateur
- Un bouton de settings: utiliser pour récupérer le dictionnaire.
- Une barre de progression: indique l’avancement de la recherche.
- Un bouton de validation: il sert à lancer la recherche du mot, il est uniquement disponible si le hash est de la bonne taille et qu’un dictionnaire est charger.
- Différents labels : pour donner des indication sur la dernière recherche (taille du dictionnaire, nombre de tentative, temps de recherche). *[5]*

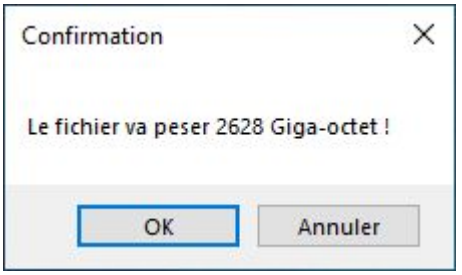
Si un résultat est retrouvé il sera affichée dans une pop-up. *[6]*

Annexes :

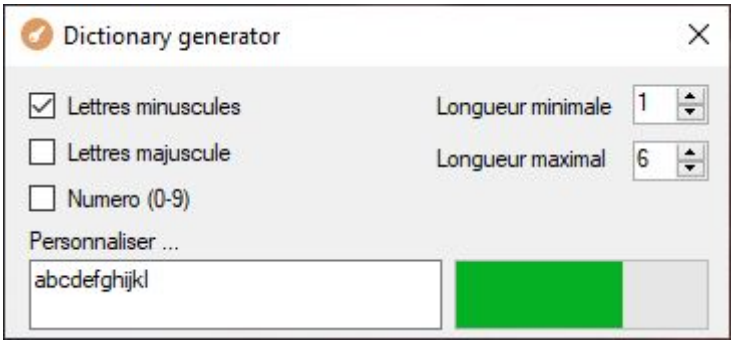
Dictionnaire:



[1] *- Application "Dictionnaire"*



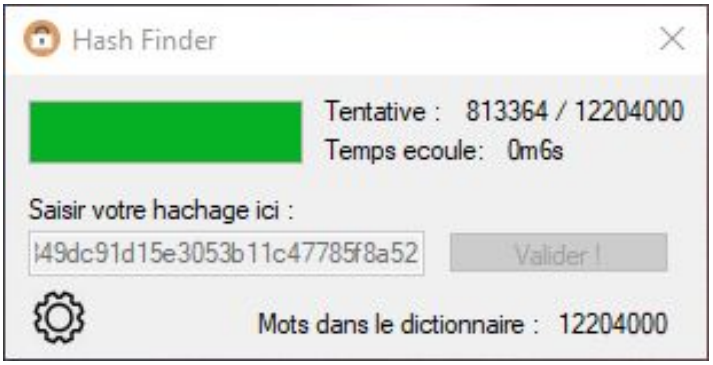
[2] *- Confirmation avec taille du fichier*



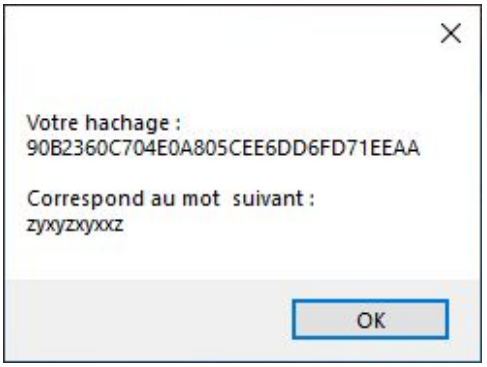
[3] *- Fichier en cour de génération*

Hachage:

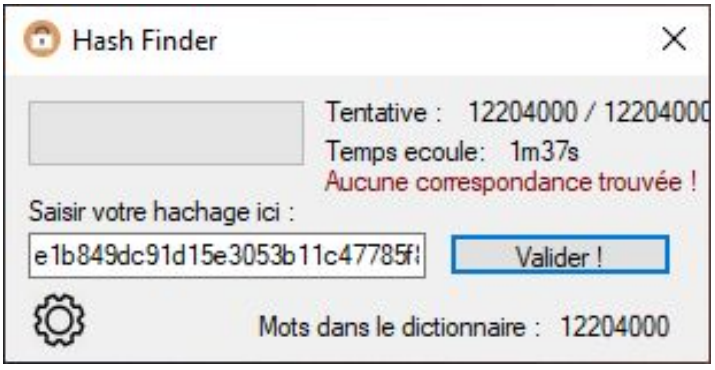
***[4]** - Application "Hachage"*



***[5]** - Information sur la recherche*



***[6]** - "Pop-up" avec résultat*



***[7]** - Aucun résultat trouvé*

Références:

[a] **MD5 C# :**
https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.md5?view=netframework-4.8

[b] **Windows Form :** https://fr.wikipedia.org/wiki/Windows_Forms

[c] **UpDownBox :**
https://docs.microsoft.com/en-us/dotnet/api/system.windows.forms.numericupdown?view=netframework-4.8

--

Code utiliser pour genere les dictionnaires :
https://www.geeksforgeeks.org/print-all-combinations-of-given-length/