UQAR

Université du Québec à Rimouski

300, allée des Ursulines, C. P. 3300, succ. A
Rimouski (Québec) G5L 3A1, CANADA
www.uqar.ca

DÉPARTEMENT DE MATHÉMATIQUES, D'INFORMATIQUE ET DE GÉNIE

Sécurité Informatique
Devoir 1 — Énoncé

SIGLE :	INF36207
TITRE :	Sécurité Informatique
GROUPE :	06
PROFESSEUR :	Steven Pigeon
	K-212
	steven_pigeon@uqar.ca
DATE DE REMISE :	23 Février 2021, avant minuit

---

0. Modalités. Vous devez faire le devoir en équipes de deux. Le devoir devra être remis par courriel, lequel contiendra une archive comprenant un document texte (.docx ou autre) qui contient les réponses (discussions, numéro bonus et mots de passes récupérés) et les programmes que vous devrez réaliser au n° **2**. Les programmes devront être fonctionnels, évidemment, et l'archive devra contenir tout ce qui est nécessaire pour les faire fonctionner (on doit pouvoir les compiler et les exécuter). Le nom de l'archive doit contenir le nom des deux coéquipiers et le numéro du formulaire : 1 . Les versions électroniques (pdf) seront aussi sur Moodle.

Notez que chaque devoir est *unique*. Le numéro 1 ne peut être utilisé que par une seule équipe. Si deux équipes utilisent le même formulaire, les deux seront disqualifiées — un euphémisme pour « auront zéro ».

1. Casser des mots de passe. 15 pts. Supposez que vous ayez capturé le fichier de mots de passe d'un système dont vous tentez de prendre le contrôle. Vous voulez obtenir les mots de passe originaux : vous devez monter une attaque contre ces mots de passe qui sont camouflés grâce à l'algorithme MD5. Les *hashes* que vous avez capturés sont les suivants :

```
79a6d9a2dc0bd42ddc52b4d61c18140a
2df3ca5c3e9f8eabc061c53da00153fa
8faf0fadf3a6df81e36d0350b24d1f67
155f6ad5aeae33b3dc50a7b7e1b06870
bc154c11b3a21546b558f0188f53c992
f14068f40d2ecc6ada7d49c47b4e239d
40e97e068bff213f9b1f94a173b82da8
4d3ff40fe2bcf4be7838f7dc4ab95702
87ab78851cf6345fb00c9f1da0d48b4a
8385b8f96c657be19dc1d47618b7ca11
b3bf1e2a1bca4239c24d04b694213089
0da24d3b8b27f13578e6324d60055a73
55cd0793487b4d922fb965afde217510
633014b47d1aff64236edde3858860d3
40d8b3d3b94d4613acc58a74c3f5c1e1
```

Pour ce qui suit, vous avez le choix du langage de programmation : Java, C, C++, C#, Python, Windows-Power Shell, Bash, etc. Cependant, pour le numéro **1 b)**, considérez un langage capable de générer du code *rapide*. De plus, les librairies qui calculent le hash MD5 sont disponibles sur toutes les plateformes et il en existe des *bindings* pour la plupart des langages, vous n'aurez donc pas à l'implémenter vous même. Quelque soit le langage que vous aurez choisi, vous devez remettre un projet complet qui montre que le code fonctionne — *pas de code, pas de points*.

a) Attaques par dictionnaire. 3 pts. Utilisez le dictionnaire `mots-8-et-moins.txt` (que vous trouverez sur Moodle) pour monter une attaque par dictionnaire contre les *hashes* ci-dessus. Donnez les mots de passe en clair récupérés.

b) Attaques par énumération. 10 pts. Vous avez remarqué que certains des *hashes* ne sont pas résolus par l'attaque par dictionnaire. Dans ce cas, vous devrez monter une attaque par énumération où vous allez générer toutes les chaînes de longueur 1, toutes les chaînes de longueur 2, toutes les chaînes de longueur 3, etc. jusqu'à ce que vous trouviez une chaîne dont le *hash* corresponde. Puisque le but n'est pas de vous faire passer de longues heures de temps de calcul, supposez que les mots de passe n'ont pas plus de 8 caractères de long, et que les caractères sont tirés de l'alphabet suivant :

```
abcdefghijklmnopqrstuvwxyz0123456789!@#$%&*
```

Donnez les mots de passe récupérés en clair.

2. Sur la complexité de casser les mots de passe. 2 pts. À la lumière du n° **2**, qu'est-ce que vous pouvez dire sur le choix d'un mot de passe ? Qu'est-ce que vous suggéreriez pour déjouer à la fois les attaques par dictionnaire et les attaques par énumération ? Quelle stratégie *simple* utiliseriez vous pour vous choisir un mot de passe sécuritaire (sans pour autant être impossible à taper) ?