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 :	INF11207
TITRE :	Sécurité Informatique
GROUPE :	06
PROFESSEUR :	Steven Pigeon
	K-212
	steven_pigeon@uqar.ca
DATE DE REMISE :	20 Février, avant minuit

— 20 —

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 convenir le nom des deux coéquipiers et le numéro du formulaire : 20 . Les versions électroniques (pdf) seront aussi sur Moodle.

Notez que chaque devoir est *unique*. Le numéro 20 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. Un chiffre simple. 2 pts. Vous avez capturé un bout de papier où on peut lire

```
FYMYRNLUNYLLYMNLYMXYJYAUMYIHNOHZUCVFYJIOLFYWUGYGVYLNYNFYVLCY
```

Pouvez vous le décrypter ?

2. Casser des mots de passe. 10 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 captués sont les suivants :

```
06e06b19b0767fa9eac324ff7b862b55
4618ce9962c71d6cd72baca7c64f48bd
a81db505516fbc98d6cb2b5b25c27eff
3dac72783f355eb5f7204a16e28581aa
67fe2162edcd031fdb94cee677d71bfc
26e06acd9b4ff54789a3d4fa28368ed6
cca1e5130e25c6aa1734899fd989db8f
664c0555fa58ce3438297f25b42e7d25
a5025fa7e30f04e9257396b4bb7106ca
08535dd077e347a53c5259e635b101d4
8d67749554704be831f82d802223c917
c332878cfbab4a42c2c16d0503ee869f
f5677fd2be37417e9b57a969bbebd7f4
2339577ebad59fa3e64d04fd2de80db4
4bf7c505cae6a66960c23e27f807d887
```

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 **2 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*.

2 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.

2 b) Attaques par énumeration. 7 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 en clair récupérés.

3. Sur la complexité de casser les mots de passe. 3 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 tapper) ?

4. Bonus. 5 pts. Utilisez l'analyse par fréquence et décryptez ce cryptogramme (par substitution simple) :