CFPT - Centre de formation professionnelle technique

ECOLE D'INFORMATIQUE

Examen M183 2.11.2021

Partie Pratique

Durée : 60 min

Matériel autorisé : Votre documentation personnelle (ce qui se trouve sur votre disque dur, théorie et exercices compris). **Attention : réseau non autorisé !**

A la fin de l'examen : zippez votre solution et nommez là ainsi « <votre nom> <votre prénom> - ExaM183». Demandez au surveillant le droit de rebrancher le réseau et rendez votre solution sur le devoir du classroom. Demandez-lui qu'il vous confirme la bonne réception de votre travail.

Consignes

Vous trouverez ci-joint le projet d'un jeu qui a de grosses lacunes en termes de sécurité. En effet, pour l'instant le meilleur score est stocké en clair dans un fichier texte à la fermeture de l'application. Il est donc très facile de modifier le score souhaité à la main. Votre mandat est de sécuriser un minimum cette partie, voici en détails ce qui vous est demandé :

- A la fermeture de l'application
  - Effectuez un hash du score avec un salt : Récupérer le hash du score (le salt doit être déclaré comme constante dans votre code et aura comme valeur « exaM183 »). Pour un score de 6, la valeur avant hash sera donc : « 6exaM183 » et le hash récupéré en utilisant la classe « MD5CryptoServiceProvider » sera « a33c4ee0b2ec9d9d193b4ce544abbbd3 ». Vous pouvez toutefois utiliser une autre classe valide de la librairie .Net si vous le préférez.
  - Encryptez le score : encryption « maison » de la façon suivante (exemple entre parenthèse avec un score de 6) :
    - Multipliez le score par 36 (36x6 = 216)
    - Ajoutez des chiffres aléatoires entre 0 et 9 tous les 2 caractères dans le score déjà mutiplié (216 peut devenir 271760)
  - Ecrivez, le hash ainsi que le score encrypté, dans le fichier texte sur 2 lignes distinctes (méthode WriteLine() du StreamWriter).

- Au chargement de l'application
  - Lisez les 2 lignes du fichier (méthode ReadLine() du StreamReader à chaque fois)
  - Decryptez le score : Il s'agit de l'opération inverse que pour l'encryption. D'abord on enlève un caractère sur 2, puis on divise par 36.
  - Vérifiez ensuite que le hash du score décrypté correspond bien à celui récupéré dans le fichier. Si c'est bon on met à jour la variable « bestScore », sinon il y a eu triche, on la laisse donc à 0.

De façon générale appliquez les bonnes pratiques vues en cours ainsi que les normes de programmation de l'Ecole. Ainsi pensez à bien regrouper votre code dans de nouvelles fonctions, notamment pour :

- Hasher le score
- Encrypter le score
- Decrypter le score

Dernière question, est-ce qu'à votre avis l'application est bien sécurisée pour autant ? Si on vous donne l'exécutable et que vous souhaitez connaître la façon dont est crypté le score afin de le modifier dans le fichier texte, comment procéderiez-vous ?
Ecrivez votre réponse dans l'en-tête de votre programme en répondant à ces 2 questions :

1. S'il existe une technique quelle est-elle ?
2. Comment s'en prémunir ?