ESIREM
ÉCOLE SUPÉRIEURE D'INGÉNIEURS
NUMÉRIQUE ET MATÉRIAUX

Contrôle Continu : Systèmes d'information avancés.
13 octobre 2020

Durée 1h, tous documents non électroniques autorisés.
Le barème est donné à titre indicatif.

---

1. (1 point) À quoi servent les systèmes de gestion de code source (git, svn, mercurial, bazaar) ?
   A. Couvrir automatiquement le code avec des tests unitaires, tests d'intégration, tests fonctionnels.
   B. Gestion des ressources du serveur.
   C. Gestion de l'historique du projet.
   D. Ralentir le développement et augmenter son prix.
   E. Permet le développement des fonctionnalités en parallèle.
2. (1 point) À quoi sert la commande `git init` ?
   A. Initialiser un dépôt Git.
   B. Vérifier l'état de l'arbre de travail.
   C. Indexer (mais pas valider) des fichiers modifiés.
   D. Valider des modifications.
   E. Introduire des conflits.
3. (2 points) Une fonction à sens unique (one-way function) c'est ...
   A. Une fonction $f : X \to \mathbb{N}$ telle que $f(x) = f(y)$ pour tout $x, y \in X$, t.q. $x \neq y$.
   B. Une fonction $f : X \to \mathbb{N}$ telle que $f(x) = x^2$ pour tout $x \in X$.
   C. Une fonction qui peut être facilement calculée, mais qui est *impossible* à inverser.
   D. Aucune des réponses précédentes n'est correcte.
4. (3 points) Donner deux exemples d'utilisation de fonctions de hachage.

Soit K une clef de chiffrement de taille n. Soit M un message de taille n à chiffrer. L'algorithme de chiffrement fonctionne comme ceci :

```
def chfrm (M, K):
  c = M
  for i in [1, 1, 2, 4, 7, 13, 24]:
    for j in range (0, i):
      # range (0,i) va générer la liste [0, 1, 2, ... , i-1]
      c = c ^ K  # ^ c'est XOR, ou exclusif
  return c
```

5. (5 points) Que pouvez-vous dire de sa fiabilité ?

Une fonction de hashage "`MyHash`" est construite par la méthode Merkle-Damgård en utilisant XOR en tant qu'une fonction de compression, avec un rembourrage par zéros. Le vecteur d'initialisation est égal à 10101111_2.

6. (2 points) Combien d'octets y a-t-il dans un bloc ?
7. (3 points) Trouver une préimage de 00111000_2.
8. (3 points) Trouver $y \neq x$ t. q. $\texttt{MyHash}(y) = \texttt{MyHash}(x)$.