Sylvain ESCASSUT
Nils FRADIN

TP2 Authentification

Exercice 1 (SHA1 (3 points))

- Calcule de SHA-1 pour les deux images
  Images 1 : img1.jpeg, on a obtenue le SHA1 suivant :
  cd4e1f42d9891d4f01e06c78d2d986223a756c05
  Images 2 : img2.png on a obtenue le SHA1 suivant :
  7fa085c8b9ee1f652b61bc901bff3aa904926292
- Après avoir converti les images nous avons calculer le SHA1 des deux pdf :
  PDF 1 : img1.pdf, on a obtenue le SHA1 suivant :
  6777c4735d9804763ad3ab55a308a1d2adc28c87
  PDF 2 : img2.pdf, on a obtenue le SHA1 suivant :
  6777c4735d9804763ad3ab55a308a1d2adc28c87

Exercice 3 (Casser des mots de passe (12 points))

1. L'algorithme de hachage utilisé est MD5, et le sel est : AAAA
2. La commande a utiliser pour vérifier le mot de passe est :
   openssl passwd -1 -salt AAAA '!!1331xxx'
   Le retour de la commande nous retourne bien le même mot de passe haché que celui de l'énoncé.
3. Pour trouver quel mots de passe sont associés au deux mot de passe haché, nous avons utiliser un bash nous permettant d'ouvrir le fichier, de parcourir les mots de passe proposer, puis de calculer le mot de passe hacher pour chaque mots de passe et de tester si ils sont identique a ces souhaiter dans l'énoncer.
   Le mot de passe associer au mot de passe hacher avec le sel BABA est : batman
   Le mot de passe associer au mot de passe hacher avec le sel CACA est : enigma

4. Pour caser les mots de passe du fichier crack-password.txt nous avons utiliser la commande : ./john chemin_du_fichier.extension

   Les règles :
   usera = lettre du clavier
   userb = capital des pays
   userc = prénom
   userd = animaux en anglais
   usere = super héros