Cryptographie avancée - TP2

Anne Garcia-Sanchez

M2i - CFA CCI Avignon, 17 septembre 2024

Fonctions de hachage cryptographiques

1 Propriétés de sécurité des fonctions de hachage

Pour comprendre les propriétés de sécurité attendue d'une fonction de hachage cryptographique, on propose d'étudier la fonction de hachage simpliste qui consisterait à calculer la somme des codes ascii des caractères d'un message. Appelons-la `asciihash`.

Exemple: `asciihash('hello')` donne 532

1. *Résistance à la pré-image*: si $\mathcal{H}$ est une fonction de hachage, étant donnée une empreinte h, il doit être calculatoirement difficile de retrouver un message m tel que $\mathcal{H}(m) = h$

   La fonction `asciihash` n'est pas une bonne fonction de hachage: chercher un mot formé de 3 lettres majuscules dont l'empreinte vaut 195.

2. *Résistance à la seconde pré-image*: étant donné un message m, il doit être calculatoirement difficile de trouver un message m' tel que $\mathcal{H}(m) = \mathcal{H}(m')$

   Soit le message `"AA"`, trouver un autre message composé de caractères imprimables (une seconde pré-image) qui donne la même empreinte avec `asciihash`.

3. *Résistance aux collisions*: il doit être calculatoirement difficile de trouver deux messages m et m' tels que $\mathcal{H}(m) = \mathcal{H}(m')$

   Trouver deux messages qui ont la même empreinte avec `asciihash`.

2 SHA-2, SHA-3

Utiliser la librairie Python `pycryptodome` pour calculer l'empreinte de `hello world` avec SHA2-224 et vérifier que l'on trouve bien `2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522a563582b`

Calculer l'empreinte de `hello world` avec SHA3-224 et vérifier que l'on trouve `dfb7f18c77e928bb56faeb2da27291bd790bc1045cde45f3210bb6c5`

Vérifier que l'on retrouve le même résultat avec les commandes linux.

3 Brute-force

On connait le haché d'un mot de passe:

`d4b19a9d2c50e189321d5ebae2c3f512e002fed309a79e5c78fae14722a178e4`

Par ailleurs on sait que ce mot de passe n'est composé que de 4 lettres.

Écrire un programme Python qui permet de retrouver le mot de passe.

On n'utilisera pas d'outil tout prêt permettant de faire cette recherche.

4 Bonus: Collision sur la fonction MD5 tronquée

Trouver deux chaînes de la forme "M2I cherche collision ????????????" qui ont des empreintes MD5 dont les 32 premiers bits sont les mêmes.

Les douze ? peuvent être n'importe quel caractère affichable, comme des chiffres par exemple.