INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Département Sécurité et Technologies Informatiques

Cryptograhie – TD4

Jérémy Briffaut <jeremy.briffaut@insa-cvl.fr>

Jean-Christophe Deneuville <jean-christophe.deneuville@insa-cvl.fr>

Lundi 1er octobre 2018

En cas de doute, référez-vous au cours 4, slides 27 et suivantes.
Téléchargez et décompressez l'archive `TD4.zip`.

Exercice 1 Définition des macros `md5`

Cet exercice est à réaliser dans le fichier `md5.h`.

1. En vous aidant de la macro `F(x, y, z)`, définir les macros pour `G`, `H`, et `I`.
2. De manière similaire, en vous aidant de `F(a, b, c, d, x, s, t)`, définir les macros pour `GG`, `HH`, et `II`.

Exercice 2 Implémentation de `md5`

Cet exercice est à réaliser dans le fichier `md5.c`.

1. *(Initialisation)* Initialisez les registres `A`, `B`, `C`, et `D` avec les valeurs suivantes :
   — `A = 0x67452301`,
   — `B = 0xefcdab89`,
   — `C = 0x98badcfe`, et
   — `D = 0x10325476`.
2. *(Ronde 1)* Appliquez la ronde 1 avec la fonction `FF` de la manière suivante : `FF(a, b, c, d, x[0], S11, 0xd76aa478)`.
3. *(Finalisation)* Comme pour le registre `A`, ajouter les valeurs `b`, `c` et `d` aux registres `B`, `C` et `D`.
4. *(Mise à jour de l'empreinte)* Mettre a jour les bits 4 à 16 du digest avec les registres `A`, `B`, `C` et `D`.

Exercice 3 Sanity check

Vous venez d'implémenter votre première fonction de hashage, félicitations ! Assurez-vous que celle-ci produit bien des sorties conformes aux spécifications en vous aidant de la fonction système `md5sum`.

Exercice 4 Fonctionnement général

Cet exercice est à réaliser dans le fichier `main.c`.

1. Donner le schéma d'appel de fonction de ce programme.
2. Compiler avec le `Makefile` fourni et tester le programme `myMD5sum`.

Exercice 5 Librairie cryptographique

Ajouter la fonction `md5` à votre bibliothèque.