Licence L2 STS Mention SPI Parcours Informatique
Unité 174EN007
Sécurité Informatique

TD2

Ce second TD porte sur l'algorithme de hachage SHA-256 et son implémentation en C (cf. implémentation de Brad Conte sur https://github.com/B-Con/crypto-algorithms).

Exercice n°1

Etudiez les principes de fonctionnement de l'algorithme SHA-256 à partir de la documentation issue de la fiche Wikipédia.

Exercice n°2

- Dans la construction de Merkle-Damgård a quoi correspond *IV* ?
- Dans le prétraitement, à quoi sert de compléter (bourrage ou *padding*) le message M ?
- Calculer la valeur de k pour le message "Hello World !" (codage ASCII étendu)
- Expliciter l'objectif et le fonctionnement de la fonction de compression.

Exercice n° 3

Rappels :

Type	Taille	Signé	Non signé
char unsigned char signed char	>= 8 bits	-127 à +127	0 à 0xFF
short signed short (défaut) unsigned short	>= 16 bits	-32 767 à +32767	0 à 0xFFFF
int signed int (défaut) unsigned int	>= 16bits (taille bus de données)	-32 767 à +32768	0 à 0xFFFF
long signed long (défaut) unsigned long	>= 32 bits	-2 147 483 647 à +2 147 483 647	0 à 0xFFFFFFFF
long long signed long long (défaut) unsigned long long	>= 64 bits	-9 223 372 036 854 775 807 à +9 223 372 036 854 775 807	0 à 0xFFFFFFFFFFFFFFFF

Pour une machine 16bits, un entier prend 16 bits, pour une machine 32 bits, un entier prend 32 bits et ainsi de suite.

Les opérations binaires sont les suivantes :

- opération binaire ∧ (AND) : &
- opération binaire ∨ (OR) : |
- opération binaire ⊕ (XOR) : ^
- complément binaire ¬ (not) : ~

(a) Etudiez l'implémentation des fonctions suivantes :

- fonction décalage binaire à gauche $ROTR^n(x)$: $(x >> n) \vee (x << (32 - n))$
- fonction décalage binaire à droite $SHR^n(x)$: $x >> n$
- fonction $Ch(x, y, z)$: $(x \wedge y) \oplus (\neg x \wedge y)$
- fonction $Maj(x, y, z)$: $(x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$
- fonction $\sum_0^{\{256\}}(x)$: $ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$
- fonction $\sum_1^{\{256\}}(x)$: $ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$
- fonction $\sigma_0^{\{256\}}(x)$: $ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$
- fonction $\sigma_1^{\{256\}}(x)$: $ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$

D'après vous, pourquoi sont-elles définies comme macros ?

(b) Etudiez l'implémentation de la fonction de compression *sha256_compress*.

Comment est implémentée la boucle *Pour i = 1 à N* de l'algorithme ?
Comment est calculée la valeur W_t ?

(c) Etudiez la fonction *sha256_compute.*

Comment se fait le découpage des données en bloc de 512 bits ?
Expliquer comment le bourrage a été implémenté.

(d) Etudiez la fonction *sha256_convert*.

Quelle est l'utilité de cette fonction ?
Donnez un exemple de fonctionnement.