Licence Informatique

Introduction à la Cryptographie

Arbres de Merkle

Gilles Dequen

1 Contexte

On souhaite expérimenter le contrôle d'intégrité de données suivant le principe de l'arbre de Merkle. Pour ce faire, vous utiliserez l'implantation de la fonction de hachage TTH_{64}^{5} que vous avez mis en œuvre au cours des séances de TD. L'implantation logicielle pour traiter cette question peut-être faite dans le langage de votre choix même si le `C/C++`, `Python` ou `Java/Kotlin` devrait être privilégiés (Proscrit : Langages propriétaires Windows). Les arbres de Merkle, tel que vu en cours, permettent un contrôle d'intégrité d'un ensemble de données (e.g. un fichier) sur la base d'une possession partielle. Ce projet va vous permettre de le vérifier.

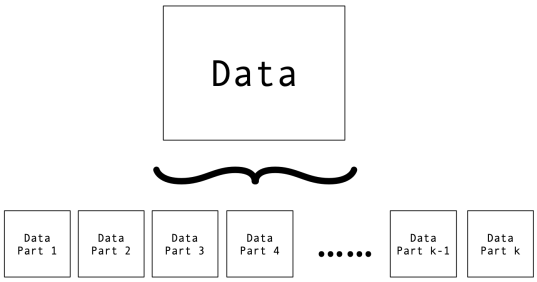
1.1 Contrôle d'intégrité

Le contrôle d'intégrité « cryptographique » suppose l'usage d'une fonction de hachage cryptographique. Ainsi, suivant l'exemple du schéma suivant, la connaissance de la valeur `0xBB3C` adjointe à `DATA` permet de contrôler son intégrité par le calcul TTH_{64}^{5}(`DATA`)$\stackrel{?}{=}$`0xBB3C`. Pour ce TP noté, `DATA` sera n'importe quel fichier de votre choix.

1.2 Partitionnement en blocs (3 pts)

`DATA` peut également être considérée comme une concaténation de blocs de données. A partir d'un fichier, et considérant des blocs de 512 octets, proposez une implantation d'un tel partitionnement. Dans le cas où la taille de votre

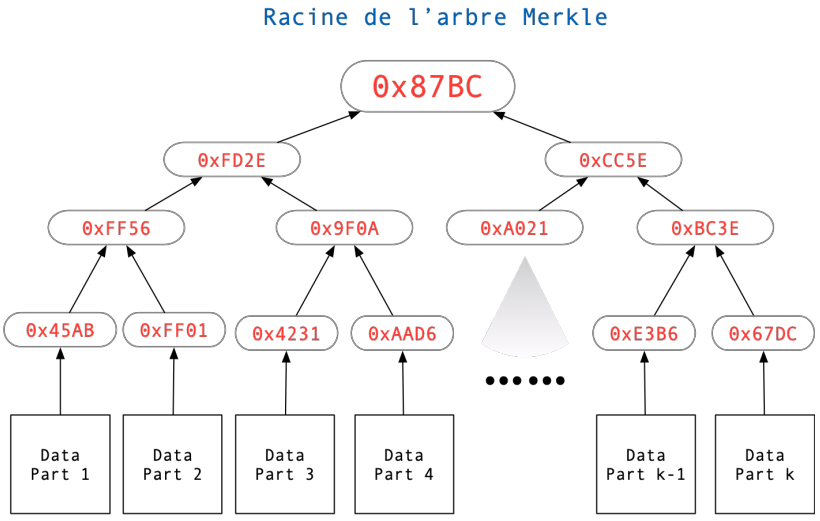
fichier à partitionner n'est pas multiple de 512, vous procèderez, à l'instar de ce que vous avez vu en TP, au bourrage du dernier bloc à 512 par le vecteur `10000000...00000`. Bien entendu, la reconstruction de `DATA` suppose, le cas échéant, le débourrage de ce dernier bloc.



1.3 Contrôle d'intégrité par parties en possédant toutes les parties (7 PTS)

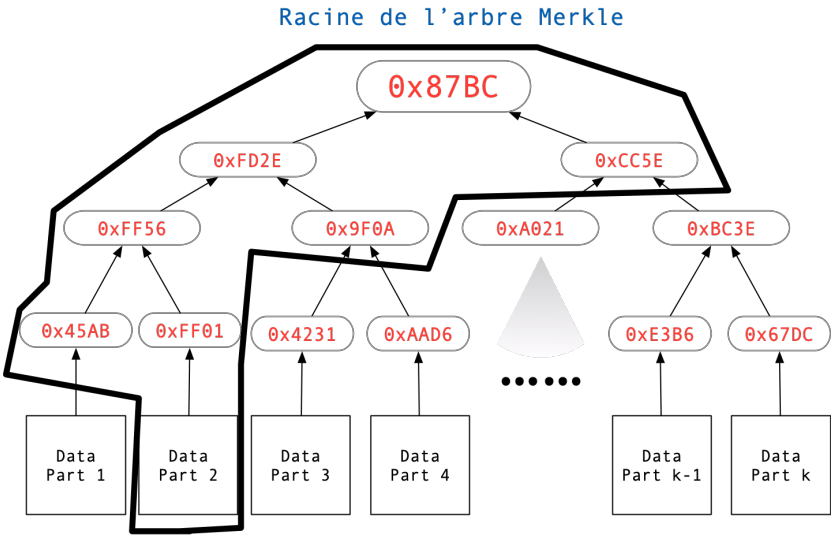
Le contrôle d'intégrité par parties permet, à partir du partitionnement en blocs de 512 octets (dans notre cas) de `DATA`, de réaliser de la même façon que précédemment un contrôle d'intégrité global de `DATA`. Cela peut-être réalisé en construisant un arbre de Merkle tel que mentionné dans la figure suivante.

Implantez le module qui calcule la racine de l'arbre de Merkle pour `DATA` en utilisant votre brique logicielle TTH_{64}^{5}.



1.4 Contrôle d'intégrité global pour une partie (10 pts)

Si l'on suppose que l'on ne considère qu'une seule partie de `DATA`, il est toujours possible de réaliser un contrôle d'intégrité global de l'information en ne considérant une quantité d'informations supplémentaire d'ordre logarithmique correspondant au empreintes « alternatives » allant de la feuille à la racine de l'arbre. Cela s'illustre dans la figure suivante pour la partie 2.



- Proposez une solution décrivant la façon dont vous intégrez les informations supplémentaires permettant le contrôle d'intégrité global pour chaque partie de `DATA` (4 pts).
- Implantez les éléments que vous proposez à votre solution et écrivez la procédure de vérification du contrôle d'intégrité (4 pts).
- Vous fournirez un jeu de test pour vos solutions (2 pts).