TP0 - Les fonctions de hachage

L'objectif de ce TP est de vous initier au concept de hachage, ainsi qu'à certaines fonctions de hachage qui vont vous servir par la suite.

[Temps estimé : ***20 ~ 30 minutes***.]

Introduction

1) Chargez dans un navigateur web le fichier ***/TP0/src/index.html***. Le navigateur doit être suffisamment récent pour pouvoir exécuter JavaScript.

Vérifiez le retour dans la console de votre navigateur.

Sur Google Chrome, et Firefox : pour vérifier que le code JavaScript de la page s'exécute correctement, tapez CTRL + MAJ + I, et ouvrez l'onglet console, et vérifiez qu'aucune erreur n'y apparait.

Si vous avez une erreur dans la console, et qu'elle semble liée au TP (elle peut aussi être liée à par exemple des extensions sur votre navigateur), faites signe à un des deux responsables de l'atelier.

2) Chargez dans un éditeur de code le TP0 à partir de son répertoire racine ***/TP0***. L'éditeur doit être capable de vous assister pour faire du code JavaScript essentiellement.

3) Rendez-vous dans le fichier du code métier ***/TP0/src/index.js*** *dans votre éditeur de code***.**

4) Allez dans la fonction **handler**, la partie du fichier où vous allez travailler pour faire les 2 exercices de ce TP.

NB : lorsqu'il est dit dans les TPs, qu'on manipule un nombre hexadécimal, c'est en fait un nombre hexadécimal **stocké en chaine de caractères**, retenez bien cette information.

Exercice 1) Le hachage sans clé

1) A l'aide de la fonction ***sha256(content)***, hachez la chaine de caractères «Hello World», et stockez le résultat dans une variable.

2) A l'aide de la fonction ***showValue(label, value)***, affichez la valeur de la variable en lui donnant un intitulé.

3) Rafraichissez la page sur le navigateur web. Que voyez-vous ?

Sur Google Chrome, et Firefox : pour rafraichir vraiment toute la page, le code HTML, ET surtout le code JavaScript associé, ne faites pas F5, mais CTRL + F5.

4) Reproduisez la 1), la 2), et la 3) pour la chaine de caractère «*Hello World!».*

5) Les valeurs des deux hachages sont-elles égales ? Qu'observez-vous ? Qu'en déduisez-vous ?

Exercice 2) Le hachage avec clé : la signature électronique

1) Toujours dans la fonction **handler**, créez-vous un couple de clé privée et de clé publique avec la fonction ***generateKeys()****, et stockez le couple de clé dans une variable.*

   La fonction ***generateKeys()*** retourne un objet JSON standard dont la structure est celle-ci :

   {

   ***privateKey** : « ma clé privée en hexadécimal (base 16) »,*

   ***publicKey** : « ma clé publique en hexadécimal (base 16) »*

   }

2) A l'aide de la fonction ***showValue(label, value)***, affichez les valeurs de vos clés privée et publique.

3) A l'aide de la fonction **en*crypt(content, privateKey)***, et de votre clé privée, chiffrez le contenu «Ma transaction», et stockez le résultat dans une variable.

4) A l'aide de la fonction ***showValue(label, value)***, affichez la valeur de la variable. Que voyez-vous ?

5) D'après vous, en quoi peut-on dire que ce contenu est signé par vous ?

6) A l'aide de la fonction ***decrypt(encryptedContent, publicKey)***, et de votre clé publique, déchiffrez le contenu chiffré plus tôt, et stockez le résultat dans une variable.

7) A l'aide de la fonction ***showValue(label, value)***, affichez la valeur de la variable. Avez-vous bien obtenu le contenu original : «Ma transaction» ?

8) Reproduisez la 6), et la 7) en essayant de déchiffrer le contenu avec une clé publique d'un nouveau couple de clé. Qu'observez-vous ? Qu'en déduisez-vous ?