CryptoQuest

L'UE de Mathématiques pour la Cryptographie va être découpée en 2 parties :

- une première partie où vous allez voir les bases mathématiques nécessaire avant de passer une partie plus pratique
- une deuxième partie plus pratique, et plus axée sur le domaine de la cryptographie

Prenez connaissance des cours avant d'entamer ce quest !

Lors du projet CryptoProject, vous allez mettre en application certaines des notions du CryptoQuest. Le CryptoProject est divisé en 3 parties distinctes. Elles auront un lien avec le chiffrement de messages et sont à faire en PHP.

- L'implémentation de l'inverse modulaire
- l'algorithme de Merkle-Hellman
- l'algorithme RSA (en bonus)

Le langage à utiliser sera le PHP.
Inutile de vous dire que vous devrez coder à la norme. Un malus sera appliqué sur la note finale en cas d'abus !
Pas de demande de validation à faire pour ce projet, il n'y aura une seule correction finale !

Inverse Modulaire

Dossier de rendu : https://rendu-svn.etna-alternance.net/v2/2018_Prep'ETNA2_CMG-MAT2_1_0-1334/CryptoProject/lagard_v/inv_mod/

Fichier à rendre : inv_mod.php

Prototype: inv_mod($a, $n);

L'inverse modulaire d'un entier relatif modulo n est un entier u tel que : a x u (mod n) = 1.
Vous allez donc écrire une fonction qui va calculer et retourner l'inverse modulaire de $a modulo $n. S'il n'y a pas d'inverse, vous retournerez 0 et afficherez le message suivant (pour changer un peu) : "Va t'acheter des doigts !".

Merkle-Hellman

Dossier de rendu : https://rendu-svn.etna-alternance.net/v2/2018_Prep'ETNA2_CMG-MAT2_1_0-1334/CryptoProject/lagard_v/merkle_hellman/

Prototypes: libre !

Maintenant que vous avez réussi à calculer l'inverse modulaire d'un nombre relatif, vous allez enfin pouvoir implémenter un algorithme. Il

s'agit entre autre de l'algorithme de Merkle-Hellman, créé il y a près de quarante ans. Vous trouverez une description de cet algorithme sur le pdf joint.
Vous êtes libre sur l'arborescence à l'intérieur du dossier demandé, mais gardez en tête que vous devez coder à la norme. Il est attendu une fonction de chiffrement et une fonction de déchiffrement, mais à vous d'étudier et de fournir ce qui est nécessaire pour les implémenter (vous pouvez donc utiliser des fonctions déjà utilisées dans le CryptoQuest par exemple).

RSA (Bonus)

À venir.