

Enoncé TP 3A IBC : Cryptographie et fonction de Hashage

TP 1 : Traitements de Cryptographie

Descriptif :

Ce TP a pour but d'orienter les étudiants de 3ème année à créer un mini site web en utilisant leurs connaissances cryptographiques.

Modalités :

Ce TP est à rendre individuellement.

Le rendu doit être sous le format d'un repository Git public.

Le lien Git est à envoyer à l'adresse mail : team@blockchain-xperts.com

L'objet du mail doit être au format : **[3A-ESGI] Cryptographie - NOM PRENOM**

Enoncé:

Créer un site web simple en Javascript qui aura comme fonction de :

- Proposer une page web formulaire pour chaque algorithme de hashage/chiffrement,
- L'utilisateur doit pouvoir chiffrer et déchiffrer des informations au choix,
- L'utilisateur doit pouvoir renseigner ses propres clés de chiffrement si nécessaire,
- Le site web doit offrir au moins les algorithmes de hashage/chiffrement suivants:
 - MD5, SHA2-256, SHA3-512, Keccak-512, RipeMD160.
 - AES, RSA, BlowFish

Le site web devra afficher toutes les informations de manière lisible et claire.

Le site web doit être déployé sur Node (version au choix, dépendant de la compatibilité).

L'usage d'un template Bootstrap afin d'accélérer la création de l'interface est recommandé.

Annexes :

<https://www.npmjs.com/package/crypto-js>

<https://www.npmjs.com/package/sha2>

<https://www.npmjs.com/package/js-sha3>

<https://www.npmjs.com/package/ripemd160>

<https://www.npmjs.com/package/node-rsa>

<https://www.npmjs.com/package/aes-js>

<https://www.npmjs.com/package/javascript-blowfish>