

FICHE : LANCEMENT "KICKOFF" DU PROJET

IDENTIFIER VOTRE CHOIX DE SUJET

Titre du projet : CryptoBib

URL si applicable : <https://www.sagemath.org/>

DÉCRIVEZ VOTRE PROJET (2 PARAGRAPHES MINIMUM)

CryptoBib serait une application desktop programmé sous le langage Python qui permettrait d'entrer un message et de choisir un type de cryptage : une méthode pour chaque sera envisagé, c'est-à-dire une méthode de cryptage symétrique, asymétrique et hybride. J'ai prévu de faire fonctionner l'application sur un environnement windows mais une application multiplateforme pourrait être envisagé.

Le message serait ainsi chiffré en interne et renvoyé à l'utilisateur. Le but sera donc de retranscrire en lignes de code les différentes méthodes de chiffrement et de l'appliquer à tous messages possibles.

L'utilisateur pourra créer des clés publiques et privées pour encoder ces différents messages.

Une interface utilisateur sera créer pour faciliter la navigation de l'utilisateur.

Le déchiffrement pourra être envisagé comme fonctionnalité de l'application en récupérant les clés permettant de déchiffrer des messages encodés par d'autres personnes.

NOMMEZ 3 COMPÉTITEURS À VOTRE PROJET

qui vous inspireront pour les fonctionnalités (avec les liens)

Nom du compétiteur 1	https://www.dcode.fr/
Nom du compétiteur 2	https://www.jetico.com/free-security-tools/encrypt-text-bctextencoder
Nom du compétiteur 3	https://calculis.net/cryptage-rsa

LISTER LE MATÉRIEL DE CE PROJET

- Ordinateur
- Connexion internet (recherche au niveau des méthodes de chiffrement)

Est-ce tous les éléments matériels nécessaires au projet sont en votre possession ? Sinon, lesquels ?

OUI

Aimeriez-vous que le département vous prête un composant, une pièce ? Si oui laquelle ?

NON

IDENTIFIER DEUX ASPECTS TECHNOLOGIQUES

Aspects : Serveurs, Services, Algorithmes, Web, IoT, etc

Aspect 1 : Application desktop Python

Aspect 2 : Cryptographie

PRÉCISEZ L'APPRENTISSAGE TECHNIQUE QUI SE FERA PENDANT LE PROJET

soyez aussi précis que possible (nom de la technologie, de la librairie, url)

Technologie : Utilisation du module de mathématiques SageMath pour Python

URL : <https://www.sagemath.org/>

Quelle utilisation en ferez-vous à l'intérieur du projet ?

Python est un très bon langage pour les projets incluant des mathématiques dû à sa simplicité et son efficacité en effet comme Python est programmé en C il hérite de la puissance de ce langage. La puissance étant un facteur non négligeable quand l'application effectue des opérations mathématiques importantes. Python s'exécutera sur un environnement desktop (windows mais une application multiplateforme pourrait être envisagé).

En ce qui concerne le module sagemath, je n'utiliserai aucune fonction pré-faites visant à crypter directement un message. Ce module ne sera utilisé que pour effectuer de opérations mathématiques :

- Création et stockage de matrices
- Opération sur des matrices (ajout, multiplication...)
- Congruences (pour les calculs mathématiques et découpage par blocs du message)
- Résolution de systèmes d'inconnus
- Autres opérations ...

Les clés seront stockées dans un fichier txt. C'est un format qui pourrait changer si un format plus sécuritaire venait à être trouvé.

ILLUSTRATION

Si une illustration peut nous aider à mieux comprendre le projet, merci de l'inclure ici.

Remplacer l'image

Vous pouvez inclure plus de matériel directement dans Github.

=> Après avoir rempli cette fiche : veuillez accepter l'assignment GitHub, convertir ce document en pdf et le remettre dans Github directement.

SVP : placer aussi le lien collaboratif du document incomplet avant de commencer.