Sprint 2 - Questions.

Comment faire si plusieurs enchérisseurs se déclarent vainqueurs ?

Un tirage au sort.

Envoie du gagnant de son chiffré signé.

Deuxième sprint, qu'attendez-vous comme documentation en anglais ?

…Sans consignes de la prof d'anglais, rien.

— *Phase d'ouverture des enchères*

1. $\mathcal{A}$ obtient $(\mathcal{C}, c, z)$ et vérifie que la signature z est valide.
2. $\mathcal{A}$ déchiffre c et calcul le second prix le plus élevé p_2 et signe ce prix p_2. La signature est notée z' et envoie p_2 et z' à $\mathcal{S}$.

Pourquoi déchiffrer c ? ce n'est pas plutôt C ?

C'est là qu'on utilise la propriété homomorphe, quand on va faire le produit de tous les chiffrés, on va obtenir la somme de tous les messages. Les messages sont encodés sous la forme b^BI.

Base

On prend l'exposant le plus élevé et le deuxième plus élevé

B nb max d'enchérisseurs possible

Que faire si la signature de A est mauvaise lorsque S vérifie ?

Annuler l'enchère.

Que faire si la signature d'un B est mauvaise lorsque S vérifie ?

Pour l'instant, nous, on le retire de la liste des enchérisseurs, on pourrait renvoyer une réponse au bidder pour que sa participation à l'enchère s'arrête là.

Arrêter tout

Si un B vérifie la signature de S et qu'elle est mauvaise, la connexion est interrompue, cela vous convient ?

Oui

Si un enchérisseur n'a pas son chiffré dans la liste et nous prévient, on garde une liste des enchérisseurs compromis ?

Que faire en cas de l'absence du chiffré ?

Pour l'instant, l'enchérisseur renvoie un message true ou false si oui ou non, il y a son chiffré dans la liste, et le vendeur renvoie un état d'exclusion aux enchérisseurs dont le chiffré est absent.

Il renvoie son prix.

Est-ce qu'on déploie les trois applications sur docker ? Ou juste le gestionnaire ?

Idéalement oui.

Demandes particulières pour l'interface graphique ?

Non